Vues de Bruxelles

Poullet, Yves

Published in:
Enjeux internationaux des activités numériques

Publication date:
2020

Document Version
le PDF de l'éditeur

VUES DE BRUXELLES. MODES ALTERNATIFS DE RÉGULATION ET LIBERTÉS DANS LA SOCIÉTÉ DU NUMÉRIQUE(257)

YVES POULLET

Professeur émérite, Université de Namur, Professeur associé à l'UCLille

1. Le fil rouge. Tant la dimension internationale d'Internet, de ses normes et de ses acteurs, que la complexité et l'évolutivité de son fonctionnement ont expliqué, des années durant, le succès de l'autorégulation comme outil possible et essentiel de la régulation de la société du numérique. L'importance de l'autorégulation ne s'est pas simplement illustrée par la création des « grands » organes de normalisation technique : l'Internet Corporation for Assigned Names and Numbers (ICANN), l'Internet Engineering Task Force (IETF), l'Internet Society Forum, le World Wide Web Consortium (W3C), l'EPC international, mais, au-delà, comme source de régulation dans nombre de domaines thématiques : le commerce électronique, la propriété intellectuelle, la protection des données, la liberté d'expression ou, à propos d'applications nouvelles : la *blockchain*, l'intelligence artificielle, la voiture connectée… Nous reviendrons largement sur ce point, cherchant dans notre introduction (Section I) à préciser chacune des notions qui permettent d'envisager les différents modes de régulation qui se proposent à propos de l'encadrement d'Internet. Nous nous arrêterons en particulier sur le choix européen privilégié : la corégulation, non sans souligner les diverses formes que la corégulation peut prendre suivant le rôle premier ou de simple accompagnateur que joue l'autorité publique.

Cette distinction de deux formes de corégulation (Section II) nous permettra, à propos de deux thématiques touchant à nos libertés dans la société du numérique : d'une part, la protection des données à caractère personnel et, d'autre part, la désinformation (les « *fake news* »), d'analyser comment l'Union européenne aborde la régulation de l'Internet au regard de la protection de nos libertés, en l'occurrence, la liberté d'expression et la protection de notre vie privée. Nous soulignerons combien

(257) L'écriture de l'article a été achevée le 5 janvier 2020. Il n'a pu tenir compte des textes, législations et jurisprudences plus récents.

les approches « régulatoires » dans ces deux domaines diffèrent profondément et combien chacune présente des risques en termes d'effectivité.

Notre dernier point concerne l'intelligence artificielle (IA) et son rôle dans la régulation. Avant d'aborder cette technologie particulière qui sans aucun doute représente l'innovation majeure du numérique, nous rappellerons, à la suite de Lessig, la vérité de l'adage « *Code is Law* », tout en soulignant la place de la technologie non comme mode de régulation séparé, mais plutôt comme outil d'effectivité de la régulation sous ces différents modes, en d'autres termes, qu'elle soit tantôt autoréglementation, corégulation ou réglementation publique. Ce rappel opéré, nous nous interrogerons sur les raisons pour lesquelles l'intelligence artificielle apparaît comme un outil à privilégier par les régulateurs, tant dans la définition du contenu de la régulation que comme instrument particulièrement efficace de l'application de celle-ci. À cet égard, nous étudierons à la fois la place que des textes récents, issus des modes de régulation tant alternatifs que législatifs confèrent à l'IA, mais également la façon dont se dessine à travers ces textes une régulation de l'IA.

Introduction. Les concepts de base : réglementation et régulation. Autorégulation *vs* corégulation (ascendante et descendante)

2. Réglementation et régulation. Cette distinction établie de longue date aux États-Unis a pénétré nos ordres juridiques européens plus récemment. On cite, à cet égard, en droit français, dès 1996, les réflexions de Timsit[258]. La distinction est claire. La régulation vise tous les procédés normatifs, peu importent leurs auteurs, privés ou publics. Ainsi, un code de conduite règle entre une ou plusieurs entreprises, voire un secteur, les relations entre elles (par exemple, bonnes pratiques anticoncurrentielles) ou entre elles et leurs clients professionnels ou non. Ainsi, la régulation vise toute norme, y compris non écrite et à portée purement sociale (comme la politesse)[259], c'est-à-dire toute prescription qui vise à harmoniser les comportements vers celui souhaité par l'auteur de la régulation, que ce comportement soit admis, encouragé ou, au contraire, fustigé et combattu par le droit. La réglementation constitue un sous-ensemble de la régulation : elle vise tous les procédés normatifs opérés par les autorités publiques constitutionnelles ou les autorités administratives (y compris indépendantes[260] auxquelles délégation de compétence normative est confiée par

(258) Ainsi, parmi ses nombreux écrits en la matière, G. Timsit, « Les deux corps du droit, essai sur la notion de régulation », *RFAP*, n° 78, avril-juin 1996, pp. 375-394.

(259) Ou la tenue vestimentaire dans une église (à cet égard, le fameux exemple de Hart à propos de la « coutume » de retirer son chapeau lors de l'entrée dans une église).

(260) Les Autorités administratives indépendantes (AAI) sont, selon le Conseil d'État (*Les autorités administratives indépendantes, rapport public de 2001*), des « organismes administratifs qui agissent au nom de l'État et disposent d'un réel pouvoir, sans pour autant relever de l'autorité du

ces autorités). En d'autres termes, elle est censée exprimer le Droit et peut s'accorder sur la place que le Droit peut accorder aux autres modes de régulation, comme il sera dit ci-après (nos 5 et s.).

Une dernière précision me semble nécessaire : il est coutume de parler de droit souple, « mou » ou « flou » selon les auteurs(261) ou, pour reprendre l'expression anglaise plus connue, de « *soft law* ». Cette expression mélange souvent des procédés de régulation non étatique, comme des codes de conduite privés et de réglementation au sens strict, car produit par l'autorité publique(262), comme les recommandations de la Commission européenne ou les codes d'éthique publiés en annexe d'une législation. Il importe de réserver le mot « Droit » aux seules sources étatiques et de souligner qu'il existe effectivement une tendance des autorités réglementaires à préférer à un droit dur, qui s'appuie sur les modes traditionnels de sanctions civiles, administratives ou publiques, un droit conçu plus comme un modèle « recommandé » pour lequel aucune sanction n'est édictée ou basé sur la récompense pour celui qui agit conformément au prescrit (ainsi, par l'octroi de primes aux bâtiments bien isolés). Cette méthode douce d'intervention du Droit est particulièrement bienvenue lorsque le domaine à réglementer est non encore stable, en particulier en considérant l'imprévisibilité des développements et impacts des futures applications technologiques(263).

L'intervention législative sous forme de législations dites « bac à sable » (*sandbox*) s'inscrit dans cette perspective : il s'agit de permettre, moyennant la définition de

gouvernement : il est communément admis et reconnu, dans la ligne d'une jurisprudence ancienne et bien établie du Conseil d'État, qu'il existe au sein de l'État des autorités autonomes, distinctes de l'administration, mais appartenant à l'État et dotées d'un pouvoir de décision […]. C'est là la reconnaissance même du principe de l'existence d'autorités administratives n'appartenant pas à la hiérarchie des administrations centrales aboutissant aux ministres ».

(261) Sur cette notion, en particulier C. Thibierge, « Le droit souple », *Rev. trim. dr. civ.*, 2003, p. 599. Il existe une certaine incertitude quant à la définition précise de ces termes. C. Thibierge distingue, pour sa part, trois acceptions de la notion du droit souple : le droit flou (sans précision), le droit doux (sans obligation) et le droit mou (sans sanction).

(262) En ce sens, « [l]e droit souple peut, au contraire, contribuer au renouvellement de l'État, par un élargissement de la gamme des moyens d'action des pouvoirs publics, dès lors que sont respectés les principes d'égalité et de non-discrimination. Le Conseil d'État, conformément à son office de gardien des droits fondamentaux et de conseil de l'administration, retient du droit souple son utilité et son effectivité au service de la relation qu'entretiennent l'administration et les usagers. L'administration y trouve de nouvelles marges de manœuvre et d'action, les usagers, de leur côté, sont placés dans une situation plus ouverte, disposant de solutions alternatives à la contrainte et dont il aura été vérifié qu'elles sont juridiquement sécurisées » (J. Richard, président-adjoint et rapporteur général au Conseil d'État, in *Le droit souple, Étude annuelle du Conseil d'État*, 2013, disponible sur le site : https://www.conseil-État.fr/ressources/etudes-publications/rapports-etudes/etudes-annuelles/etude-annuelle-2013-le-droit-souple).

(263) « *While there is no precise definition, a regulatory sandbox is, broadly speaking, a framework within which innovators can test business ideas and products on a "live" market, under the relevant regulator's supervision, without fear of enforcement actions in case it is determined that their business model does not comply with existing regulations. This "safe space" is usually subject to certain restrictions, typically focused on ensuring the protection of consumers, including a limited amount of time for testing* » (K. Agarwal, « Playing in the regulatory sandbox », *NYUJLB*, January 8, 2018, disponible sur le site : https://www.nyujlb.org/single-post/2018/01/08/Playing-in-the-Regulatory-Sandbox).

balises, certaines expérimentations, de soumettre ces dernières à contrôle et de prévoir des réglementations définitives à la suite de rapports et débats publics. Pour ne reprendre que le domaine du numérique, on citera en ce sens les législations « bac à sable » en matière de voitures connectées(264) ou de « *blockchains* »(265).

Ainsi, les documents et textes d'autorégulation, mode alternatif de régulation que nous allons aborder, ne peuvent être qualifiés de Droit, même si, comme nous le montrerons, ils peuvent trouver leur origine dans une règle de droit, voire être appuyés par eux. Leur contenu, leur prononcé, la qualité de leurs auteurs et leurs sanctions peuvent de même être balisés par le Droit et, en toute hypothèse, être soumis au contrôle des tribunaux, le Droit se réservant le « pouvoir du dernier mot ».

3. Autorégulation *vs* corégulation (ascendante et descendante)(266). L'autorégulation se définit par l'adoption volontaire par une entreprise ou un groupe

(264) On note ainsi, en Belgique : proposition de résolution relative au lancement de projets pilotes « véhicules motorisés » (*driverless cars*), *Doc. parl.*, Ch. repr., sess. ord. 2014-2015, n° 54-687/1 ; proposition de résolution relative aux véhicules autonomes, Rapport fait au nom du Comité d'avis des questions scientifiques et technologies par M. Jef Van Den Bergh, *Doc. parl.*, Ch repr., sess. ord. 2016-2017, n° 54-2096/1 ; résolution relative aux véhicules autonomes, *Doc. parl.*, Ch. repr., sess. ord. 2016-2017, n° 54-2096/2 ; le Code belge de bonnes pratiques d'expérimentation des véhicules autonomes sur la voie publique est disponible sur : https://mobilit.belgium.be/fr/resource/code_de_bonnes_pratiques_vehicules_autonomes. Il s'inspire du Code établi par le *UK Department for Transport* : « The pathway to driverless cars: a code of pratice for testing – Moving Britain ahead », 2015, disponible à l'adresse suivante : https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/446316/pathway-driverless-cars.pdf ; arrêté royal du 18 mars 2018 relatif aux essais des véhicules automatisés, *M.B.*, 19 avril 2018 ; art. 59/1 de l'arrêté royal du 1er décembre 1975 portant règlement général sur la police de la circulation routière et de l'usage publique, *M.B.*, 9 décembre 1975.
En France, voy. l'ordonnance n° 2016-1057 du 3 août 2016 relative à l'expérimentation de véhicules à délégation de conduite sur les voies publiques, *J.O.R.F.*, n° 0181 du 5 août 2016. Disponible sur : https://www.legifrance.gouv.fr/eli/ordonnance/2016/8/3/DEVR1615137R/jo/texte.

(265) Y. Poullet et H. Jacquemin, « *Blockchain* : une révolution pour le droit ? », *J.T.*, 2018, p. 818. Sur cette manière de procéder face à une innovation dont on a quelque peine à juger des risques et bénéfices et son application à la *blockchain*, lire l'excellent *paper* de M. Finck, « *Blockchain Regulation* », Max Planck Institute for innovation and Competition Research Paper nos 17 et 18, 2017. Lire également les réflexions de J. Maupin, « Mapping the global legal landscape of blockchain and other distributed ledger technologies », CIGI (Center for international Innovation Governance), Paper n° 149, octobre 2017 : « *The term sandbox here takes its cue from the Financial Conduct Authority's (FCA's) recent initiative to set up a UK regulatory sandbox: a safe space in which fintech companies targeting UK markets can test out new technologies within a "light touch" regulatory environment under close government supervision and for a defined period* ». En langue française, mêmes réflexions, in N. Deviller, « Jouer dans le "bac à sable" réglementaire pour réguler l'innovation disruptive : le cas de la technologie de la chaîne des blocs », *Rev. trim. dr. com.*, 2017, pp. 1037 et s. ; T. Verbiest, « Technologie de registres distribués : premières pistes de régulation », *RLDI*, 2016, n° 129, p. 52 ; L. de Meneval et S. Poirot, « La *blockchain*, un nouveau paradigme pour le numérique », *Expertises*, 2017, pp. 51 et s.

(266) Pour plus de détails, nos réflexions, in Y. Poullet, « Technologies de l'information et de la communication et "co-régulation" : une nouvelle approche ? », *Liber amicorum Michel Coipel*, Bruxelles, Kluwer, 2004, p. 173 ; Y. Poullet, « How to regulate Internet? New paradigms for internet governance », in J. Berleur *et al.* (éd.), *Variations sur le droit de la société de l'information*, Cahier du CRID, n° 22, 2002, pp. 130 et s. Voy. égal. T. Kleist et C. Palzer, *La corégulation, instrument moderne de régulation*, document de travail préparatoire à la conférence d'experts organisée dans le cadre de la

d'entreprises de règles qu'elles entendent respecter et, le cas échéant, des moyens par lesquels ces règles seront effectivement respectées. Des qualifications différentes y réfèrent : codes d'éthique, codes de conduite, *Privacy policies*, *Terms of reference*, *Best Practices*, etc. Ces autorégulations peuvent couvrir des domaines aussi différents que la publicité, la protection des consommateurs, la concurrence loyale, la vie privée, la lutte contre les *Fake news*, la protection des mineurs, etc. Elles peuvent être le fait d'une association professionnelle et prennent alors une dimension importante dans la mesure où elles concernent une majorité, voire l'ensemble des prestataires d'un secteur professionnel, ainsi, par exemple, les règles en matière de publicité sur Internet adoptées par l'*Online Behavioural Association*, les *Bitcoin rules*, les règles adoptées en matière de protection des enfants par l'Alliance « *Safer Social Networking Principles* », promue par l'Union européenne et qui regroupe les plateformes de réseaux sociaux ou, en matière d'intelligence artificielle, le « *Partnership on AI to benefit People and Society* », qui regroupe, outre les GAFAM, des associations, y compris de libertés civiles, et entend développer des *best practices* quant au développement et à l'utilisation des systèmes d'intelligence artificielle.

On souligne que l'autorégulation, non seulement, définit des contenus normatifs, mais, en outre, s'appuie de plus en plus souvent sur des mécanismes assurant une véritable effectivité au respect de ce contenu. Ces mécanismes sont développés par le marché et contribuent au développement d'une nouvelle économie. À cet égard, on souligne le rôle des mécanismes de labellisation et de certification(267) dont le contrôle est plus ou moins prégnant (ainsi, *e-Trust, BBBonline, Trusted shops*)(268), mais également l'existence de mécanismes privés de règlements des litiges extrajuridictionnels (les *Alternative Dispute Resolution Mechanisms* [ADR]) intervenant *on line* ou non, dans un domaine précis ou non, comme médiateurs ou arbitres. Ces ADR, souvent plus accessibles aux personnes victimes dans un contexte international, moins coûteux et disposant d'un « personnel » plus adéquat, énoncent des sanctions originales dont l'effet dissuasif est supérieur à celui lié au prononcé des décisions des tribunaux : le retrait du label, la publicité de la décision prise par l'ADR et/ou, enfin, l'exclusion du groupe. Bref, l'autorégulation se présente comme un système normatif

présidence allemande de l'UE : « Plus de confiance dans les contenus. Le potentiel de la corégulation et de l'autorégulation des médias numériques », Leipzig, du 9 au 11 mai 2007, disponible sur http://www.leipzig-eu2007.de/fr/downloads/dokumente.asp.

(267) C. Connolly, « Benchmarks for global privacy standards », *Working Paper*, novembre 2009, Pyrmont. On distinguera les labels et certificats américains comme Trust-e (http://www.etrust.org/) : « *A PrivacyTrust Certification indicates that your website has been reviewed by PrivacyTrust and has met our stringent privacy and data protection requirements. Having a PrivacyTrust Seal on your website signifies to customers that any critical data collected, suchas home addresses and phone numbers are not exchanged with third parties without their consent. This is vital in having a trustful relationship between you and your customers* ». Parmi les labels en matière de *privacy*, on cite BBBonLine ; Webtrust (www.webtrust.org/) ; ou, européens, comme EURO PRISE (https://www.european-privacy-seal.eu/.../5e13d520-1af0-4af0-a5a.) ; *e-PRIVACY* (https://www.eprivacy.eu/fr/labels-de-protection) ou *Trusted Shops* (www.trustedshops.be/fr/label-de-qualite/protection-acheteur.html), moins centrés sur la question de la protection des données à caractère personnel.

(268) Ces mécanismes sont souvent liés à un code de conduite dont le mécanisme de certification et l'attribution d'un label ont pour but de vérifier le respect et d'attester l'effectivité de ce code de conduite.

complet fixant les mécanismes de création de la norme, son contenu, ses modes de contrôle, ses « juges »[269] et ses sanctions, et présentant des avantages indéniables par rapport à des réglementations publiques et leurs acteurs juridictionnels moins adaptés, étant donné la dimension internationale d'Internet et les exigences d'une réponse rapide, non contestable et effectivement suivie.

4. L'accord interinstitutionnel de 2003 « Mieux légiférer »[270] consacre ces modes alternatifs de régulation (les MAR), mais assigne à leur reconnaissance par le Droit certaines conditions (voy. *infra*, n° 4). Par cet accord, les trois institutions s'engagent à améliorer la qualité de la législation européenne ainsi que sa transposition en droit interne. Elles reconnaissent également que l'Union européenne ne doit légiférer que « dans la mesure nécessaire, conformément au protocole sur l'application des principes de subsidiarité et de proportionnalité » et s'engagent à recourir, dans les cas appropriés, à des mécanismes de régulation alternatifs plutôt qu'à un acte législatif. L'article 16 justifie ainsi le recours aux méthodes alternatives de régulation : l'autorégulation et la corégulation. L'article 18 de l'accord définit la *corégulation* comme « le mécanisme par lequel un acte législatif communautaire confère la réalisation des objectifs définis par l'autorité législative aux parties concernées reconnues dans le domaine (notamment les opérateurs économiques, les partenaires sociaux, les organisations non gouvernementales ou les associations) ». Pour être précis, il s'agit d'une corégulation descendante, puisque, si la synergie entre les actions de régulation des autorités publiques et des pouvoirs privés est ainsi consacrée, c'est bien dans le cadre de l'action législative qui en fixe les balises et doit limiter là son action que la régulation privée doit intervenir.

Par ailleurs, certaines qualités sont exigées des instruments de régulation privée. L'article 16 de l'Accord exige, en effet, premièrement, la légitimité des auteurs, ce qui implique au moins la consultation des parties intéressées par l'objet de la réglementation (par exemple, les consommateurs en matière de réglementation de la publicité ou de transactions *B to C*), et la transparence des règles adoptées par les auteurs ; en deuxième lieu, la conformité du contenu, c'est-à-dire le respect par les textes privés des balises fixées par le texte réglementaire ; en troisième lieu, l'effectivité des mesures prises par les pouvoirs privés qui doivent aider au respect des règles fixées par l'autorité publique et, donc, représenter une plus-value à l'instrument législatif.

5. De la corégulation descendante comme mode préféré de régulation par l'Europe. C'est le modèle de la corégulation descendante qui se trouve privilégié par la Commission européenne et, de manière plus large, par les autorités européennes[271], en particulier dans le domaine du numérique. La réglementation européenne en matière d'Internet fourmille d'applications de ce modèle de la

(269) Ainsi, récemment, l'annonce par Facebook de la création d'un « tribunal » propre qui jugera de l'ensemble des litiges nés de comportements sur son réseau social.

(270) *J.O.*, C 321 du 31 décembre 2003, pp. 1-5.

(271) Le Comité économique et social européen identifiait déjà, en 2005, les conditions de bon exercice de l'autorégulation et de la corégulation, en louant cette dernière méthode de régulation : prise en compte de l'intérêt général, transparence, représentativité et efficacité du suivi. Voy. Comité économique et social européen, *L'état actuel de la corégulation et de l'autorégulation dans le marché unique*, mars 2005, p. 12.

corégulation, qu'on songe notamment à la directive « Commerce électronique » de juin 2000, qui « promeut » la conclusion de codes de conduite et les ADR ; à la directive « *Copyright Act at the Electronic Age* », qui laisse aux plateformes le soin de définir les moyens de répondre aux exigences de la directive, les textes en matière de contenus illégaux ou dommageables qui renvoient à des codes de conduite à prendre par les plateformes ou à la directive sur les services de médias audiovisuels, directive revue en 2018(272). Le RGPD, en particulier, constitue une parfaite application de cette approche corégulatrice, car il promeut, en ses articles 40 et suivants, la reconnaissance et l'encadrement de divers modes d'autorégulation privés comme les codes de conduite, la certification, les règles d'entreprise contraignantes et les mécanismes extrajuridictionnels de solutions des litiges. On note que le RGPD entend également, avec son principe de « *Privacy by design* », imposer à la technologie elle-même le respect de ses dispositions. Nous reviendrons sur ce point lors de notre analyse des relations entre technologie et droit (*infra*, n° 16). L'article 4*bis* de la directive « audiovisuel » récemment modifiée est clair : « Les États membres encouragent l'utilisation de la corégulation et la promotion de l'autorégulation au moyen de codes de conduite adoptés au niveau national dans les domaines coordonnés par la présente directive, dans la mesure où leur ordre juridique le permet. Ces codes : a) sont conçus de manière à être largement acceptés par les principaux acteurs dans les États membres concernés ; b) définissent leurs objectifs clairement et sans ambiguïté ; c) prévoient que la réalisation de ces objectifs est suivie et évaluée de manière régulière, transparente et indépendante ; et d) assurent une mise en œuvre effective, notamment au moyen de sanctions efficaces et proportionnées ». Le point 3 de cet article 4*bis* prévoit l'éventualité d'une intervention plus stricte ou détaillée des États membres, notamment « lorsque leurs autorités ou organismes de régulation nationaux indépendants concluent qu'un code de conduite ou des parties de celui-ci se sont avérés ne pas être suffisamment effectifs »(273).

Terminons nos réflexions sur le modèle de la corégulation descendante en soulignant la difficulté pour la Commission européenne d'imposer ce modèle. Ainsi, en matière de lutte contre la désinformation – les *fake news* –, la Communication de la Commission européenne en date d'avril 2018 « *Tackling online disinformation: an European Approach* » se heurte, selon le rapport récent de la Commission, à la difficulté de vérifier et donc d'imposer les principes de la Communication aux signataires

(272) Directive (UE) 2018/1808 du Parlement européen et du Conseil du 14 novembre 2018 modifiant la directive 2010/13/UE visant à la coordination de certaines dispositions législatives, réglementaires et administratives des États membres relatives à la fourniture de services de médias audiovisuels (directive « Services de médias audiovisuels »), compte tenu de l'évolution des réalités du marché, *JOUE*, L 303/69 du 28 novembre 2018. Sur ce cas, lire le rapport IRIS-Special 19 remis au Conseil de l'Europe : A. Arena, M. D. Cole *et al.*, *Self- and Co-regulation in the new AVMSD*, Publication de l'*European Audiovisual Observatory*, Strasbourg, 2019.

(273) Directive (UE) 2010/13/UE du Parlement européen et du Conseil du 10 mars 2010 visant à la coordination de certaines dispositions législatives, réglementaires et administratives des États membres relatives à la fourniture de services de médias audiovisuels (directive « Services de médias audiovisuels »), telle que modifiée par la directive (UE) 2018/1808 du Parlement européen et du Conseil du 14 novembre 2018, L 303, p. 69.

du *Code of Practice on Disinformation*, qui rassemble les principales plateformes de communication et d'information, de même que les associations de régie publicitaire.

6. RGPD et *Code of Practice on Disinformation* – Corégulation ascendante et descendante. Notre propos entend ainsi opposer deux modes de corégulation. Dans le cadre du RGPD, il est indiscutable que les principes de la protection des données ont été fixés par le législateur européen, voire, au-delà, leur interprétation est confiée à l'organe institutionnel créé par le RGPD : le Comité européen de contrôle (EDPB), dont la mission est décrite comme suit : « Le comité veille à l'application cohérente du présent règlement »(274). Si la prééminence de l'État dans l'œuvre de régulation est évidente dans le RGPD, il n'empêche que la section 5 du chapitre IV intitulé « Responsable du traitement et sous-traitant » leur consacre cinq longs articles (art. 40 à 44) : « Les États membres, les autorités de contrôle, le comité et la Commission encouragent l'élaboration de codes de conduite destinés à contribuer à la bonne application du présent règlement, compte tenu de la spécificité des différents secteurs de traitement et des besoins spécifiques des micro, petites et moyennes entreprises »(275). Clairement, il s'agit d'attribuer aux instruments alternatifs un rôle subsidiaire, d'adaptation des principes légaux aux particularités d'un secteur ou d'une entreprise, sans pouvoir y déroger, mais afin d'assurer à ces principes le maximum d'effectivité. Il s'agit clairement d'une corégulation descendante.

À l'inverse, le cas du « *Code of Practice on Disinformation* » illustre une tout autre approche. Certes, l'initiative de lancer la discussion revient à la Commission européenne qui non seulement a lancé une consultation en 2017, mais en plus a réuni un *High Level Group of Experts on Disinformation* dont elle a adopté le rapport. À la suite de la parution de la Communication de la Commission européenne ainsi que du rapport du groupe d'experts de haut niveau et dans l'optique de lutter contre la désinformation en ligne, certaines des plus importantes plateformes en ligne (Facebook, Google, Twitter, Mozilla et Microsoft(276)), les annonceurs ainsi que l'industrie publicitaire – suivant la voie de l'autorégulation certes suggérée dans les travaux du

(274) L'article 70 du RGPD liste pas moins de vingt-cinq domaines de compétences de l'EDPB. En particulier, il revient à l'EDPB : « b) de conseiller la Commission sur toute question relative à la protection des données à caractère personnel dans l'Union, y compris sur tout projet de modification du présent règlement ;
c) de conseiller la Commission, en ce qui concerne les règles d'entreprise contraignantes, sur la forme de l'échange d'informations entre les responsables du traitement, les sous-traitants et les autorités de contrôle, ainsi que les procédures qui s'y rapportent ;
d) de publier des lignes directrices, des recommandations et des bonnes pratiques sur les procédures de suppression des liens vers des données à caractère personnel, des copies ou des reproductions de celles-ci existant dans les services de communication accessibles au public, ainsi que le prévoit l'article 17, paragraphe 2 ;
e) d'examiner, de sa propre initiative, à la demande de l'un de ses membres ou à la demande de la Commission, toute question portant sur l'application du présent règlement, et de publier des lignes directrices, des recommandations et des bonnes pratiques afin de favoriser l'application cohérente du présent règlement [;] ».
(275) Art. 40.1 RGPD. L'article 42 relatif aux « certifications, labels, etc. » exprime le même principe.
(276) Alors que les quatre premières sociétés étaient présentes à l'origine de l'adoption du Code en 2018, Microsoft a rejoint la liste des signataires en mai 2019.

Groupe – ont adopté le *Code of Practice on Disinformation*[277]. On ajoute que la Commission européenne, prise de court par cette initiative des acteurs eux-mêmes, a enjoint alors aux signataires de ce code de bonnes conduites à lui remettre des rapports actualisés pour « documenter » la manière dont ils assurent la conformité aux engagements qu'ils ont pris[278]. En octobre 2018, les auteurs du Code précisaient: « *The Signatories agree to* cooperate *with the European Commission in assessing the reporting on the functioning of the Code. This cooperation may include: Making available appropriate information upon request; Informing the Commission of the signature or withdrawal of any Signatories; responding to the Commission's questions and consultations; Discussing the above-mentioned assessment and reports in meetings of the Signatories; and inviting the Commission to all such meetings* ».

La technologie, et en particulier l'intelligence artificielle (IA/AI en anglais), comme mode de régulation ou comme garantie d'effectivité des régulations ? Qu'il s'agisse du RGPD ou du *Code of Practice on Disinformation*, la régulation, au sens le plus large, y compris la réglementation, fait appel à la technologie pour rendre plus effectives les dispositions qu'il entend voir respecter. Ainsi, les principes du « *privacy by design* » ou « *privacy by default* » à propos du RGPD et la demande formulée par le *Code of Practice* de mettre au point des systèmes d'IA capables de repérer des montages d'images ou la présence de *chatbots* traduisent la manière dont le droit réclame le relais de la technologie. Comment situer dès lors les relations entre régulation et technologie ? On connaît la phrase célèbre de Lessig : « *Code is Law* »[279]. Par rapport à cette affirmation, nous souhaitons analyser la manière dont ces deux textes, mais également d'autres textes récents comme la directive relative au droit d'auteur dans la société digitale et le règlement sur les relations loyales, définissent le rôle de la technologie, en principe non comme une source d'un contenu normatif supplémentaire, mais comme une manière d'assurer l'effectivité de la réglementation en question. Nous verrons par ailleurs que le Droit peut imposer précisément pour cette raison cette technologie.

Cette lecture des textes cités aboutira à quelques constatations : la première concerne l'attention tout à fait particulière donnée aux systèmes d'intelligence artificielle qui, au-delà des technologies traditionnelles, s'avèrent d'une grande efficacité

(277) Commission européenne (DG Connect), « Code of Practice on Disinformation », le 26 septembre 2018, mis à jour le 17 juin 2019, disponible sur https://ec.europa.eu/digital-single-market/en/news/code-practice-disinformation, consulté le 30 août 2019.

(278) Commission européenne, « Questions and Answers – Code of Practice against disinformation: Commission calls on signatories to intensify their efforts », le 29 janvier 2019, disponible sur : https://europa.eu/rapid/press-release_MEMO-19-752_en.htm, consulté le 30 août 2019 ; Commission européenne (DG Connect), « Statement on the Code of Practice against disinformation: Commission asks online platforms to provide more details on progress made », le 28 février 2019, disponible sur : https://ec.europa.eu/digital-single-market/en/news/statement-code-practice-against-disinformation-commission-asks-online-platforms-provide-more, consulté le 30 août 2019. Précisons que, de janvier à mai 2019, la Commission européenne a assuré un suivi mensuel des actions entreprises par les signataires pour se conformer aux engagements pris dans le *Code of Practice on Disinformation*. Voy. *ibid*.

(279) L. Lessig, *Code, and Other Laws of Cyberspace*, New York, Basic Books, 2000, disponible sur le site : http://code-is-law.org.

et mieux adaptés à donner leur pleine effectivité à la régulation ; la deuxième analyse la dérive ou plutôt la crainte de voir, au nom de leur effectivité, les systèmes technologiques devenir subrepticement source de nouveaux contenus de régulation ; troisièmement, certains textes, comme la récente résolution de la Commission européenne à la suite des travaux du *High Level Group on AI*[280], mettent sur pied certains éléments d'une régulation de l'intelligence artificielle (IA).

Deux modèles différents de corégulation : le RGPD et le *Code of Practice on Disinformation*

Section 1.
La corégulation et le RGPD

7. Le RGPD ou un modèle de corégulation descendante. La section 5 du chapitre IV intitulé « Responsable du traitement et sous-traitant » du RGPD consacre cinq longs articles (art. 40 à 44) aux modes alternatifs de régulation. On note la référence du règlement aux besoins particuliers des petites et moyennes entreprises[281] qui, selon les auteurs du RGPD, trouveraient dans ces mécanismes une façon aisée de satisfaire aux prescrits réglementaires. Il est vrai que les codes de conduite constituent une solution mutualisée adéquate pour des entreprises qui ne peuvent se permettre d'investir la matière de la protection des données et définir elles-mêmes leur politique en la matière[282]. En ce qui concerne la directive 95/46/CE aujourd'hui abrogée, un seul article, l'article 27, ouvrait la voie à la reconnaissance de ces instruments : l'article mentionnait la possibilité pour les entreprises de se référer à des codes de conduite. En particulier, la directive incitait ces dernières à développer ces codes au niveau européen et à les faire agréer par les autorités de protection des données, voire au niveau européen par le Groupe de l'article 29. Cette entrée timide des

(280) High Level Group of Experts on AI, *Ethics Guidelines for trustworthy AI Systems*, décembre 2018, publié par la Commission après commentaires le 9 avril 2019, disponible sur le site : https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai.

(281) « Les États membres, les autorités de contrôle, le comité et la Commission encouragent l'élaboration de codes de conduite destinés à contribuer à la bonne application du présent règlement, compte tenu de la spécificité des différents secteurs de traitement et des besoins spécifiques des micro, petites et moyennes entreprises » (art. 40.1 RGPD). Même encouragement à propos de la certification et des labels à l'article 42.1.

(282) Notons que ces entreprises sont dispensées de la nomination d'un délégué à la protection des données imposée aux grosses entreprises et dont le rôle est précisément d'aider en interne l'entreprise à définir sa politique en matière de protection des données et les moyens de sa réalisation (sur cette fonction et ses missions, lire les articles 38 et 39 du règlement).

modes alternatifs de régulation en 1995 fait place, vingt et un ans après, à une affirmation plus explicite et plus large de l'intérêt de ces mécanismes, sans pour autant déboucher, loin de là, sur le système américain qui prône une solution principalement autorégulatrice de la protection des données(283). En effet, le système européen, s'il admet des méthodes alternatives de régulation en subordonne la légitimité à une stricte conformité à la loi et ne les envisage en définitive que comme moyen de lui ajouter des précisions et, bien évidemment, une effectivité renforcée. On ajoute que, pour renforcer encore ce contrôle des autorités publiques et, en particulier, des autorités nationales et de l'EDPB, (European data Protection Board), ce dernier a émis des « *guidelines* » en la matière(284), balisant encore un peu plus les conditions mises au contenu et aux mécanismes d'agrément mis en place par le RGPD.

8. Différents types de mécanismes d'autorégulation. Différents types de mécanismes d'« autorégulation » sont promus par le règlement : les codes de conduite (art. 40), la certification (art. 42), en ce compris les labels(285), et les « procédures extrajudiciaires et autres procédures de règlement des litiges » que le règlement invoque incidemment(286), là où la défunte directive se contentait d'évoquer les seuls codes de conduite. Par ailleurs, le règlement prend soin de préciser, en son article 40, l'étendue de leur objet possible, depuis le traitement loyal jusqu'à la notification aux autorités de contrôle. Sans vouloir reprendre ici les commentaires déjà publiés à propos de chacune de ces formes d'autorégulation, nous souhaitons ici montrer comment les balises, mises par le RGPD à ces divers instruments, démontrent le souci d'une corégulation particulièrement forte et destinée à assurer le respect des trois conditions de validité imposées aux modes alternatifs de régulation par l'accord interinstitutionnel, rappelées ci-dessus au n° 4, à savoir la conformité du contenu, la légitimité des auteurs et l'effectivité du mode alternatif de régulation choisi.

(283) De manière critique sur la solution de l'autorégulation en matière de vie privée aux États-Unis, lire R. Gellman et P. Dixon, « Failures of privacy self-regulation in the United States », in D. Wright et P. De Hert (eds), *Enforcing Data Protection*, Springer, 2016, pp. 53 et s. ; voy. égal. l'étude très fouillée et comparative de nombreuses *Privacy Policies* et de leurs ambiguïtés, J. Reidenberg, J. Bhatia, T. Breaux et T. Norton, « Ambiguity in privacy policies and the impact of regulation », *Journal of Legal Studies*, 2016, vol. 43, pp. 163 et s.

(284) Les *Guidelines 1/2019 on Codes of Conduct and Monitoring Bodies underRegulation 2016/679* (4 juin 2019) et l'*Opinion 9/2019 on the Austrian data protection supervisory authority draft accreditation requirements for a code of conduct monitoring body pursuant to article 41 GDPR* (9 juillet 2019), documents disponibles sur le site de l'EDPB.

(285) Pour une analyse plus fouillée sur la situation existant avant le RGPD, nous nous référons à l'étude complète réalisée par le CRIDS pour l'Union européenne : F. de Villenfagne, F. Dumortier et Y. Poullet, *Comparison of Privacy and Trust Policies in the Area of Electronic Communications: final Report*, 2007, Namur, disponible à l'adresse : http://www.crid.be/pdf/public/5596.pdf ; *cf*. également, sur un jugement critique sur ces modes de régulations dans leur utilisation en matière de protection des données, O. Tambou, « L'introduction de la certification dans le règlement général de protection des données à caractère personnel : quelle valeur ajoutée ? », *RLDI*, 2016/126, n° 3986, pp. 43 et s.

(286) On retrouve la référence aux modes alternatifs de règlement de litiges dans l'énumération des objets des codes de conduite (art. 40.2) au point k) : « les procédures extrajudiciaires et autres procédures de règlement des litiges permettant de résoudre les litiges entre les responsables du traitement et les personnes concernées en ce qui concerne le traitement, sans préjudice des droits des personnes concernées au titre des articles 77 et 79 ».

9. Conformité, légitimité et effectivité des MAR dans le RGPD. La conformité se déduit de la définition même du rôle du MAR choisi : il s'agit, dit l'article 40.2, pour le code de conduite de « spécifier » le règlement (art. 40.2). On ajoute que l'approbation et le contrôle par des organismes agréés par les APD (art. 41) et les organes de certification (art. 43) ont précisément pour but cette vérification de conformité. Les MAR doivent constituer un plus par rapport aux prescrits du RGPD. C'est sans doute sur la deuxième condition de validité des modes alternatifs de normativité aux yeux du droit que le RGPD se montre le plus silencieux. On note, dans le considérant 99, que les codes de conduite doivent « si possible [être] pris après consultation » des personnes concernées ou, plutôt, de leurs représentants (ce peuvent être des associations de liberté civile ou de consommateurs). Quant à l'effectivité, elle est omniprésente dans le RGPD, il s'agit des exigences de publicité données par l'APD aux MAR souscrits ou obtenus, mais, surtout, les pouvoirs accordés par les MAR (art. 40.4) tant aux organismes agréés par les APD qu'à ceux d'accréditation acceptés par ces mêmes APD (art. 41.4 et 43.4)[287]. Les lignes directrices déjà citées fixent les points sur lesquels ces organismes agréés doivent porter leur attention. Ainsi, ces derniers vérifieront les traitements couverts par les MAR, les justifications apportées par le ou les responsables du traitement quant au choix de la méthode de régulation ; ils s'inquiéteront de la représentativité des porteurs du projet de MAR et de la qualité des consultations opérées en particulier vers les *stakeholders* et les personnes concernées. Leur approbation d'un MAR répondra aux critères suivants : le besoin de recourir à cette méthode de régulation ; l'effectivité de l'application du RGPD ; la spécificité du contenu au regard des principes du RGPD ; les garanties appropriées de fonctionnement du système mis en place et, enfin, les mécanismes de surveillance effectifs par l'organe de contrôle et l'APD. On ajoute que le RGPD assigne une véritable responsabilité à ces organismes dans le suivi du MAR, de même que des pouvoirs de vérification, voire de retrait d'agrément, autant de devoirs qu'ils devront exercer. On ajoute que les mécanismes de labellisation et de certification ajoutent encore à l'effectivité des dispositions du RGPD par des sanctions originales propres à ces mécanismes : tantôt l'infraction aux règles amène le retrait du label sans plus ; tantôt s'ajoutent une amende et/ou, surtout, la publicité de la décision motivée via une *blacklist*. Les promoteurs de ces certifications sont généralement des associations privées travaillant dans un marché concurrentiel, ce qui, selon certains auteurs, risque de les mettre dans une position délicate lorsqu'il s'agit de « sanctionner » un client.

(287) L'agrément ou accréditation de ces organismes (volontaire s'il s'agit de s'occuper uniquement de codes de conduite, obligatoire s'il s'agit de certification ou de labels) est lui-même sévèrement contrôlé par les APD, et doit répondre aux exigences fixées par les lignes directrices et l'opinion déjà citées de l'EPDB. Ainsi doivent être vérifiés l'indépendance de fonctionnement de l'organisme (nécessité de règles formelles pour la nomination, procédures et fonctionnement de l'organe de contrôle qui peut cependant être un organe interne au responsable du traitement), son indépendance financière, organique et organisationnelle ; son respect du principe d'*accountability* et la présence de règles quant aux conflits d'intérêts ; l'expertise des membres de l'organe ; la transparence des règles quant au déroulement de la procédure à la suite d'une plainte ; le lien avec l'APD ; l'existence d'un rapport périodique ; l'obligation de répondre et d'information auprès des personnes concernées ; les mécanismes de révision du code monitoré.

10. Les MAR dans le cadre des flux transfrontières. Notre propos se limitera aux deux principales innovations en matière de reconnaissance des MAR : la première est la consécration, par le règlement en ses articles 47 et suivants, des « règles d'entreprise contraignantes », création du Groupe de l'article 29 et jusque-là sans fondement législatif(288) ; la seconde concerne les modifications apportées à la reconnaissance européenne des codes de conduite *made in US*, dans le cadre du « *Privacy Shield* » (le « bouclier européen en matière de protection des données ») qui, à la suite de l'arrêt *Schrems*, a succédé au défunt « *Safe Harbor* »(289).

Reconnues dès 2007 de façon prudentielle par le Groupe de l'article 29(290), les règles d'entreprise contraignantes (ou « BCR » pour *Binding Corporate Rules*) sont un instrument juridique européen auquel une société multinationale ou un groupe d'entreprises peut recourir afin de garantir un niveau adéquat de protection des données à caractère personnel lors du transfert de ces données, au sein du groupe, au départ d'un pays situé dans l'Union européenne (UE) ou dans l'Espace économique européen (EEE) vers un pays tiers. Cette consécration législative va de pair avec des balises supplémentaires mises à ce mécanisme alternatif que sont les règles d'entreprise. Ainsi, le règlement précise d'emblée que les règles d'entreprise ne pourront être validées qu'à la triple condition, premièrement, qu'elles aient suivi la procédure de cohérence des articles 63 et suivants, qui soumettent le projet de règles à l'avis du Comité européen de protection des données (EDPB), deuxièmement, qu'elles soient juridiquement contraignantes pour les entreprises de même, ajoute le règlement,

(288) Ces documents sont publiés sur le site du Groupe de travail « Article 29 » (http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083). Ces deux documents prennent soin de fixer les règles transitoires et interprètent la notion de garanties appropriées reprise au texte des articles 47 et suivants, notamment en distinguant ce qui doit être partie intégrante des règles telles qu'elles devront être publiées et ce qui doit accompagner la demande introduite auprès des autorités de contrôle. On note en particulier l'ajout de dispositions relatives à la transparence et l'engagement de voir les recours fixés sur le territoire de l'Union européenne, lorsqu'un membre du groupe d'entreprises est situé en Europe. Les deux documents ont été finalement approuvés le 18 avril 2018 : *Recommendation on the Approval of the Controller Binding Corporate Rules Form* (WP 264) et *Recommendation on the Approval of the Processor Binding Corporate Rules Form* (WP 265), disponibles sur le site du Groupe de travail « Article 29 » : http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623848.67. Les recommandations citées précisent que les engagements contenus dans les règles dites « contraignantes » nées de l'adoption par le groupe d'entreprise doivent générer des droits opposables devant les juridictions des pays des personnes concernées. Il revient par ailleurs au groupe de démontrer que les personnes concernées pourront, en vertu d'une sorte de « stipulation pour autrui », bénéficier de l'engagement pris envers l'autorité de contrôle.

(289) Décision 2000/520/CE relative à la pertinence de la protection assurée par les principes de la sphère de sécurité et par les questions souvent posées y afférentes publiées par le ministère du Commerce des États-Unis d'Amérique, *J.O.C.E.*, 25 août 2000, I, 215, pp. 7-47.

(290) Voilà la liste des *Working Papers* du Groupe de travail « Article 29 » relatifs aux règles d'entreprise : WP 107 : *Working Document Setting Forth a Co-Operation Procedure for Issuin – Common Opinions on Adequate Safeguards Resulting From « Binding Corporate Rules »* ; WP 108 : *Working Document Establishing a Model Checklist Application for Approval of Binding Corporate Rules* ; WP 133 : *Recommendation 1/2007 on the Standard Application for Approval of Binding Corporate Rules for the Transfer of Personal Data* ; WP 153 : *Working Document setting a table with the elements and principles to be found in Binding Corporate Rules* ; WP 154 : *Working Document Setting up a framework for the structure of Binding Corporate Rules* ; WP 155 : *Working Document on Frequently Asked Questions (FAQ) related to Binding Corporate Rules*.

que pour leurs employés et, enfin, troisièmement, que, sur cette base, les personnes concernées jouissent de droits opposables devant les tribunaux. L'article 49.2 décrit le contenu minimal de tout projet de règles contraignantes et ne se contente pas d'introduire les nouveautés explicites du règlement comme l'exigence d'un délégué, des engagements en ce qui concerne le profilage, etc. On note, en particulier, que la responsabilité des entités présentes sur le territoire européen est affirmée, sauf preuve contraire apportée par celles-ci, pour toute violation du règlement, peu importe la localisation du membre du groupe d'entreprises(291) et que des mécanismes d'audit et de réception des plaintes doivent exister dans le groupe d'entreprises(292).

La CNIL présente comme suit le « *Privacy Shield* » ou « bouclier de protection des données » : « Le Bouclier de Protection des Données, mieux connu sous le nom de *Privacy Shield*, est un mécanisme d'auto-certification pour les entreprises établies aux États-Unis qui a été reconnu par la Commission européenne comme offrant un niveau de protection adéquat aux données à caractère personnel transférées par une entité européenne vers des entreprises établies aux États-Unis. Ce mécanisme est par conséquent considéré comme offrant des garanties juridiques pour de tels transferts de données ». La décision européenne de remplacer la décision de 2000 dite « *Safe Harbor Principles* », prise après des négociations difficiles avec les États-Unis entamées dès le printemps 2015, s'expliquait non seulement par la délicate question du droit des autorités publiques américaines d'opérer des surveillances de masse auprès des responsables de traitement, ce qui entraîna le recours victorieux de Max Schrems auprès de la Cour de Luxembourg, mais également par les faiblesses du système d'autorégulation mis en place aux États-Unis et son manque d'effectivité(293). Le *Privacy Shield*(294) entend remédier à ces imperfections, même s'il respecte la difference

(291) Art. 47, 2, f) : « l'acceptation, par le responsable du traitement ou le sous-traitant établi sur le territoire d'un État membre de sa responsabilité pour toute violation des règles d'entreprise contraignantes par toute entité concernée non établie dans l'Union ; le responsable du traitement ou le sous-traitant ne peut être exonéré, en tout ou en partie, de cette responsabilité que s'il prouve que le fait générateur du dommage n'est pas imputable à l'entité en cause [;] ».

(292) Art. 47, j) : « les mécanismes mis en place au sein du groupe d'entreprises, ou du groupe d'entreprises engagées dans une activité économique conjointe pour garantir que [*sic*] le contrôle du respect des règles d'entreprise contraignantes. Ces mécanismes prévoient des audits sur la protection des données et des méthodes assurant que des mesures correctrices seront prises pour protéger les droits de la personne concernée. Les résultats de ce contrôle devraient être communiqués [au délégué à la protection des données et à l'autorité de contrôle] ».

(293) Pour une analyse fouillée du *Privacy Shield* et de la protection adéquate ou non qu'il offre, voy. C. de Terwangne et C. Gayrel, « Flux transfrontières de données et exigence de protection adéquate à l'épreuve de la surveillance de masse. Les impacts de l'arrêt *Schrems* », *op. cit.*, pp. 53-73.

(294) Annexe 2 de la décision européenne, 12 juillet 2016, EU-U.S. Privacy Shield Framework Principles Issued by The U.S. Department of Commerce, disponible sur le site du *Privacy Shield*, https://www.privacyshield.gov/Program-Overview. La décision de la Commission a été prise le 12 juillet 2016 et est en vigueur depuis le 1er août de cette même année. Sur cette décision et les documents y afférents, voy. le site de la CNIL : https://www.cnil.fr/fr/le-privacy-shield. Voy. égal. l'avis du Groupe de travail « Article 29 » sur le projet déposé, par la Commission en février 2016, et les critiques adressées à ce projet de texte : « *Although the WP29 does not expect the Privacy Shield to be a mere and exhaustive copy of the EU legal framework* ; *it considers that it should contain the substance of the fundamental principles and as a result, ensure an "essentially equivalent" level of protection* » (http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2016/wp238_en.pdf).

d'approche américaine, principalement d'autorégulation, et l'approche européenne, principalement legislative : « *While the United States and the European Union share the goal of enhancing privacy protection for their citizens, the United States takes a different approach to privacy from that taken by the European Union. The United States uses a sectoral approach that relies on a mix of legislation, regulation, and self-regulation* ». Nonobstant ce rappel d'une distinction fondamentale quant au mode de régulation, le *Privacy Shield* affirme, comme le faisait déjà le *Safe Harbor* à propos de la directive, les mêmes principes de base que le règlement européen. Quant au mécanisme de contrôle du respect des principes énumérés, proposé par le *Privacy Shield*, il reprend le mécanisme d'autocertification déjà mis en place par le *Safe Harbor*, mais l'adapte quelque peu en tenant compte des critiques adressées par la Commission, à la suite de l'arrêt de la Cour de justice(295). Sans doute, peut-on voir dans l'accord nouveau un renforcement du contrôle *a priori* des engagements des organisations et entités lors de leur demande d'adhésion au *Privacy Shield*, en particulier non seulement l'engagement du *Department of Commerce* américain de vérifier l'*accuracy* du code de conduite des entreprises par rapport à la réalité, mais, au-delà, pour assurer le suivi de ces engagements, l'obligation d'introduire dans les codes de conduite des mécanismes effectifs de recours et de sanctions(296), l'engagement du *Department of Commerce* d'entamer des investigations en cas de plaintes pour non-conformité, de même que la collaboration avec les autorités européennes de protection des données. Par ailleurs, la liste des entreprises certifiées tenue par le *Department of Commerce* fera l'objet de révisions annuelles afin de veiller à sa fiabilité. L'ensemble de ces précisions entend répondre aux lacunes décelées par la Commission européenne et rappelées ci-dessus. Ce renforcement du contrôle par la Commission témoigne de la volonté exprimée par l'Europe de ne plus se satisfaire d'un système d'autorégulation sans contrôle effectif des autorités publiques américaines

(295) Voy. l'analyse du rapport et des défaillances du système américain, C. Conolly et P. Van Dijk, « Enforcement and reform of the EU-US safe harbor agreement », in D. Wright et P. De Hert (eds), *Enforcing Privacy*, Springer, 2016, pp. 261 et s.

(296) Voy. en particulier le texte de l'annexe II du *Privacy Shield* (pt 7) : « *a. Effective privacy protection mustinclude robust mechanisms for assuring compliance with the Principles, recourse for individuals who are affected by non-compliance with the Principles, and consequences for the organization when the Principles are not followed. At a minimum such mechanisms must include:*
i. readily available independent recourse mechanisms by which each individual's complaints and disputes are investigated and expeditiously resolved at no cost to the individual and by reference to the Principles, and damages awarded where the applicable law or private-sector initiatives so provide;
ii. follow-up procedures for verifying that the attestations and assertions organizations make about their privacy practices are true and that privacy practices have been implemented as presented and, in particular, with regard to cases of noncompliance; and
iii. obligations to remedy problems arising out of failure to comply with the Principles by organizations announcing their adherence to them and consequences for such organizations. Sanctions must be sufficiently rigorous to ensure compliance by organizations.
b. Organizations and their selected independent recourse mechanisms will respond promptly to inquiries and requests by the Department for information relating to the Privacy Shield. All organizations must respond expeditiously to complaints regarding compliance with the Principles referred by EU Member State authorities through the Department. Organizations that have chosen to cooperate with DP As, including organizations that process human resources data, must respond directly to such authorities with regard to the investigation and resolution of complaints ».

et le contrôle des autorités européennes de protection des données, et rejoignent nos réflexions à propos de la corégulation en vigueur en Europe[297].

Section 2.
Le *Code of Practice on Disinformation* : une forme très allégée de corégulation

11. Le problème des *fake news* ou de la désinformation en ligne[298]. Internet a été présenté comme un espace public, une « foire aux idées », où chacun

(297) À preuve, les rapports annuels dressés par la Commission sur le respect du *Privacy Shield* par les entreprises américaines. Le rapport publié par la Commission moins d'un an après la mise en œuvre du *Privacy Shield* (*Report From the Commission to the European Parliament and the Council on the First Annual Review of the Functioning of The EU–U.S. Privacy Shield*, Bruxelles, 18 octobre 2017, COM(2017) 611 final) est optimiste à cet égard : « *The certification process has been handled in an overall satisfactory manner and more than 2400 companies have been certified so far. The U.S. authorities have put in place the complaint-handling and enforcement mechanisms and procedures to safeguard individual rights. This includes also the new additional redress avenues for EU individuals such as the arbitration panel and the Ombudsperson mechanism. Regarding the latter, an Acting Ombudsperson was designated following the change of Administration in January 2017, whereas the nomination of a permanent Ombudsperson is pending. Cooperation with European data protection authorities has been stepped up.* » Sans doute, le rapport pointe encore dix améliorations souhaitables dans le fonctionnement du processus, parmi lesquelles on relève que la publication des certificats des entreprises devra suivre et non précéder la révision qui sera opérée par le *Department of Commerce*, à la suite de l'adoption des *Privacy Shields.* Le *Department of Commerce* est, en outre, appelé à prendre des mesures proactives de contrôle du respect des engagements des entreprises, à développer sa politique d'information sur les règles du *Privacy Shield* et sa coopération avec les autorités européennes. Enfin, la question des systèmes automatisés de décision et de l'adéquation de la protection offerte aux États-Unis devra, toujours selon le même rapport, être approfondie. De manière plus récente, le rapport de l'avocat général à propos de l'affaire dite *Schrems* (concl. Av. gén. M. Henrik Saugmandsgaard Øe présentées le 19 décembre 2019, aff. C-311/18) où l'avocat général met clairement en cause l'adéquation (l'équivalence substantielle) des *Privacy Shields* exigée par l'article 45 du RGPD : « Au vu de ces considérations, il n'est pas certain que, sur la base des éléments exposés dans la décision "bouclier de protection des données", les mesures de surveillance fondées sur l'article 702 du FISA s'accompagnent de garanties, relatives à la limitation des personnes susceptibles de faire l'objet d'une mesure de surveillance et des objectifs pour lesquels des données peuvent être collectées, substantiellement équivalentes à celles qui sont requises en vertu du RGPD, lu à la lumière des articles 7 et 8 de la Charte » (n° 301).

(298) Il eût été intéressant de se pencher par ailleurs sur le cas un peu différent de la régulation des messages racistes et de xénophobie sur l'Internet. L'Europe avait procédé d'une autre manière, puisque, dès 2009, elle prenait une décision-cadre. Pour la mise en acte de cette décision, elle a proposé aux plateformes (les mêmes que celles signataires du Code sur la désinformation) un code de conduite, dont la mise en œuvre est soumise à évaluation. La dernière évaluation a eu lieu en 2016 : « *Today, the European Commission publishes the first evaluation of how IT companies applied the code of conduct to combat illegal online hate speech. The code was agreed with the IT companies (Facebook, Google (YouTube), Twitter and Microsoft) on 31 May 2016. Initial results show that 28% of all notifications of alleged illegal online hate speech lead to the removal of the flagged content.*

s'exprimerait librement et dialoguerait avec autrui. Pourtant, à cette image positive et enthousiasmante, s'est progressivement substituée, à la faveur des technologies de l'intelligence artificielle, des *chatbots* et des *nudges*, la crainte d'un Net dominé par quelques acteurs : les GAFAM, capables de nous manipuler et nous profilant tous et chacun. Sur la Toile se multiplient les discours parfois haineux et racistes et le repli sur soi « dans des bulles informationnelles (*filter bubbles*) à la faveur des partages et des algorithmes ou encore la surcharge d'informations (infobésité) dont le sens se dilue dans l'abondance et la redondance »(299). Ces craintes et constatations amènent l'Europe à agir. On peut citer nombre d'initiatives en la matière(300). Nous nous attarderons sur l'analyse de son action vis-à-vis des *fake news*(301) ou, selon l'expression préférée par le Groupe d'experts nommé par la Commission européenne, la « désinformation » (*disinformation*).

La « désinformation en ligne » est définie par ce groupe d'experts(302) comme « toute forme d'informations erronées, inexactes ou trompeuses conçues, présentées

However, only 40% of all notifications are currently reviewed under 24 hours, while the aim of the code of conduct is to review the majority within 24 hours. Commissioner for Justice, Consumers and Gender Equality Věra Jourová said: "It is our duty to protect people in Europe from incitement to hatred and violence online. This is the common goal of the code of conduct. The last weeks and months have shown that social media companies need to live up to their important role and take up their share of responsibility when it comes to phenomena like online radicalisation, illegal hate speech or fake news. While IT Companies are moving in the right direction, the first results show that the IT companies will need to do more to make it a success." As part of the code of conduct IT companies pledged to review valid removal notifications against their community guidelines and where necessary national laws transposing the Framework Decision *on combating racism and xenophobia in less than 24 hours and to remove or disable access to content, if necessary. 12 NGOs based in 9 EU countries have analysed the responses to notifications over a period of six weeks. The findings indicate that among the 600 notifications made in total, 28% lead to a removal, 40% of all responses were received within 24 hours while another 43% arrived after 48 hours* ».

(299) M. Hanot et A. Michel, « Entre menaces pour la société et risques réglementaires : les *Fake news*, un danger pour la démocratie », in Actes du colloque tenu à Namur le 28 novembre 2019, *Cahier du CRIDS*, n° 50, à paraître.

(300) Sur ces différentes initiatives européennes, lire l'excellente étude dirigée par C. Marsden et T. Meyer pour le compte de l'European Parliamentary Research Service (EPRS) et la STOA (Scientific Foresight Unit), *Regulating Disinformation with Artificial Intelligence*, EPRS, European Parliamentary Research Service Scientific Foresight Unit (STOA) PE 624.279 – March 2019. Les deux auteurs soulignent le role des théories de l'économie du comportement dans la construction des « *Business models* » développés par les géants du Net : « *Behavioural or "nudge" regulation has become a favoured "light touch" regulatory technique in the last decade. The use of behavioural psychology insights to observe changes in the "bounded rational" choices of consumers is commonplace in the online environment. Nudging was so familiar to internet regulatory school…* ».

(301) Communication de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions – Lutter contre la désinformation en ligne : une approche européenne, COM(2018) 236 final, 26 avril 2018.

(302) European Commission (Directorate-General for Communication Networks, Content and Technology), *A multi-dimensional approach to disinformation: Report of the independent High level Group on fake news and online disinformation*, Luxembourg, Publications Office of the European Union, 2018, pp. 5 et 10. Sur les raisons du choix de la notion de désinformation et de sa définition, lire M. Hanot et A. Michel, « Entre menaces pour la société et risques réglementaires : les *Fake news*, un danger pour la démocratie », *op. cit.*

et promues pour intentionnellement causer un préjudice public ou à des fins lucratives »[303].

Le scandale *Cambridge Analytica* et les rumeurs, fondées ou non, suivant lesquelles les élections américaines qui ont conduit à la victoire de Trump ou le référendum du Brexit auraient été faussés par des manipulations de l'opinion publique, ont justifié la volonté d'intervention de certains gouvernements et de la Commission européenne. Ces manipulations, venues ou du moins attribuées à des forces étrangères, agissent via les réseaux sociaux grâce à une connaissance fine tant des préférences politiques des internautes profilés grâce à des systèmes d'intelligence artificielle que des méthodes de fonctionnement de ces réseaux ou plateformes d'informations, en particulier des méthodes de *rankings*[304]. Cependant, si, incontestablement, ces actions de désinformation mettent en cause nos démocraties[305], l'intervention réglementaire s'avère délicate. La difficulté de distinguer information erronée, opinion, parodie et désinformation n'est pas chose aisée, et une intervention malencontreuse et hâtive apparaîtrait facilement comme une atteinte à la liberté d'expression, voire une censure. On rappelle le célèbre attendu de la Cour de Strasbourg dans l'affaire *Handyside c. Royaume-Uni*, la liberté d'expression « vaut non seulement pour les "informations" ou "idées" accueillies avec faveur ou considérées comme inoffensives ou indifférentes, mais aussi pour celles qui heurtent, choquent ou inquiètent l'État ou une fraction quelconque de la population. Ainsi le veulent le pluralisme, la tolérance et l'esprit d'ouverture sans lesquels il n'est pas de "société démocratique" »[306]. Ce risque est d'autant plus grand vu les craintes de censure exprimées par d'aucuns, sachant que les autorités publiques ne voient pas toujours d'un bon œil les critiques et les harcèlements des médias et journalistes[307].

(303) « *All forms of false, inaccurate, or misleading information designed, presented and promoted to intentionally cause public harm or for profit* » (HLGE, rapport cité, p. 5). Le *Code of Practice on Disinformation* qui, finalement, mettra en œuvre (voy. *infra*, n° 13) ce rapport d'experts et la Communication de la Commission retiennent la définition suivante : « *As provided under the Commission's Communication, for the purpose of this Code, the Commission as well as the High Level Expert Group in its report define "Disinformation" as "verifiably false or misleading information" which, cumulatively, (a) "Is created, presented and disseminated for economic gain or to intentionally deceive the public"; and (b) "May cause public harm", intended as "threats to democratic political and policymaking processes as well as public goods such as the protection of EU citizens' health, the environment or security". The notion of "Disinformation" does not include misleading advertising, reporting errors, satire and parody, or clearly identified partisan news and commentary, and is without prejudice to binding legal obligations, self-regulatory advertising codes, and standards regarding misleading advertising* ».

(304) A. Marwick et R. Lewis, *Media Manipulation and Disinformation Online*, Data and Society Research Institute, 2017, disponible sur le site : https://datasociety.net/pubs/oh/DataAndSociety_MediaManipulationAndDisinformationOnline.pdf.

(305) Sur ce point, A. Rangappa, « Disingformation, democracy and the rule of law », disponible sur le site : http://defusingdis.info/category/essays/, january, 30, 2019.

(306) Cour eur. D.H., arrêt *Handyside c. Royaume-Uni*, 7 décembre 1976, req. n° 5493/72, § 49. Voy. égal. Cour eur. D.H., arrêt *De Haes et Gijsels c. Belgique*, 24 février 1997, req. n° 19983/92, § 46 ; Cour eur. D.H., arrêt *Özgür Gündem c. Turquie*, 16 mars 2000, req. n° 23144/93, §§ 57 et 60.

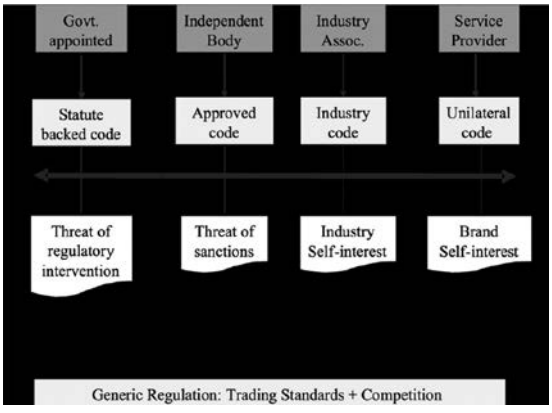
(307) À ce propos, Déclaration conjointe du Rapporteur spécial des Nations unies sur la promotion et la protection du droit à la liberté d'opinion et d'expression, du Représentant de l'Organisation pour la sécurité et la coopération en Europe (OSCE) pour la liberté des médias, du Rapporteur spécial de

Mais la manipulation ne vient pas seulement des acteurs traditionnels, mais bien également d'autres acteurs largement méconnus qui, intentionnellement, souhaitent manipuler, pour des raisons diverses, politiques au sens le plus large mais également économiques (dénigrement d'un concurrent). Leurs messages véhiculent de fausses informations présentées comme vraies et « croustillantes » ; ils pénètrent les réseaux sociaux ; utilisent les méthodes de *ranking* des plateformes (par exemple, en créant, artificiellement par des *chatbots,* des marqueurs représentant l'« intérêt » du public à ces messages) et déclenchent ainsi la référence à ces « *news* » par les moteurs de recherche ou les réseaux sociaux, alimentant ainsi les discussions entre internautes (phénomène dit de la bulle de filtre). La circulation du message sera d'autant plus aisée que les discours véhiculés trouvent écho auprès de personnes qui y retrouvent leurs propres convictions (*filterbubbles*) et se hâtent de les transférer à leurs amis, voire au-delà, d'autant plus que l'information présente l'attrait de la nouveauté et du sensationnel (phénomène dit de la chambre d'écho).

12. De la régulation européenne de la désinformation. Le rapport Millwood-Hargrave[308] de 2007 relatif à la désinformation dans les médias distinguait déjà diverses possibilités de régulation du phénomène de la désinformation. À la suite de ce premier rapport, une étude récente présentée au Parlement européen[309]

l'Organisation des États américains (OEA) pour la liberté d'expression, du Rapporteur spécial sur la liberté d'expression et l'accès à l'information de la Commission africaine des droits de l'homme et des peuples (CADHP), *op. cit.*, p. 1 : « Les autorités publiques dénigrent, intimident et menacent les médias, notamment en affirmant que ces derniers sont "l'opposition" ou qu'ils "profèrent des mensonges" et ont un agenda politique caché, ce qui accroît le risque de menaces et de violences contre les journalistes, sape la confiance du public dans le journalisme dans son rôle de "chien de garde public", et peut induire le public en erreur en brouillant les lignes entre la désinformation et les contenus médiatiques qui contiennent des informations pouvant faire l'objet de vérifications indépendantes ».

(308) M. Millwood-Hargrave, Report for Working Group 3 of the Conference of Experts for European Media Policy, More Trust in Content – The Potential of Co- and Self-Regulation in Digital Media, Leipzig: 9-11 May 2007.



(309) STOA, *Regulating Disinformation with Artificial Intelligence*, EPRS European Parliamentary Research Service Scientific Foresight Unit (STOA) PE 624.279 – March 2019, pp. 60-61.

présentait comme suit les différentes options possibles de régulation(310) du phénomène de la désinformation dans le monde de l'Internet. Ces possibilités vont depuis l'autorégulation sans aucun contrôle jusqu'à l'adoption d'une législation avec agrément des méthodes utilisées par les plateformes pour lutter contre la désinformation provoquée par les *fake news*.

Pour revenir à l'attitude européenne en la matière, notons qu'à la suite d'une enquête lancée en 2017, qui révélait que sur les trois mille réponses reçues, 97 % des répondants estimaient avoir déjà été confrontés aux *fake news*(311), la Commission lance et nomme un « Groupe d'experts de haut niveau sur le phénomène de la désinformation » (*High Level Group on Disinformation*), chargé de produire des recommandations en la matière. Le rapport du Groupe d'experts européens(312) de janvier 2018 a largement inspiré la position européenne exprimée dans la Communication : « *Tackling online disinformation: a European approach* »(313). Le rapport plaide en faveur d'une autorégulation contrôlée(314).

La position de la Commission ne s'écarte pas de cette option. Elle entend cependant affirmer quatre principes qui doivent guider son contrôle de l'autorégulation. Le premier est celui de la transparence, vis-à-vis des internautes, de l'origine, de la production, de la diffusion, du ciblage et de la sponsorisation des informations. L'identification et la traçabilité des sources de désinformation sont également réclamées au nom de cette transparence due. Le deuxième principe insiste sur l'importance d'une offre diversifiée d'informations aux citoyens de l'Union européenne pour les encourager à prendre « *des décisions éclairées guidées par l'esprit critique* », ce qui implique, ajoute la Commission, l'éducation aux médias et un journalisme de qualité. La qualité des informations véhiculées dans les réseaux sociaux est la troisième préoccupation de la Commission qui suggère à ce propos des outils tels que les indicateurs

(310) Soit : « *Option 1: Non-audited self-regulation, with increasing industry-government coordination, but no sanction on those companies choosing not to cooperate in standards; • Option 2: Audited self-regulation, under which for instance the code of practice on disinformation would be subjected to formal published audit by a commonly agreed self-regulator.; • Option 3: A formal self-regulator, recognized by the European institutions and ideally with funding separate from the industry.; • Option 4: Formal co-regulation, in which the regulator is independent from government yet subject to prior approval of codes of conduct, systems for funding and arbitration.; • Option 5: Statutory regulation, in which a regulator is tasked to combat disinformation directly by licensing of content providers and their systems for content moderation. Current electoral and broadcast regulators already perform this function for offline media* ».

(311) À côté de cette consultation publique, la Commission a également fait procéder à un sondage – *Eurobaromètre* – dans les vingt-huit États membres entre le 7 et le 9 février 2018. Ce sondage révèle que les sources d'informations en ligne sont perçues, par les citoyens européens, comme beaucoup moins fiables que les sources provenant de médias traditionnels.

(312) Rapport de l'UE « *High LevelGroup of Experts on Disinformation* », publié par la Commission européenne : European Commission (Directorate-General for Communication Networks, Content and Technology), *A multi-dimensional approach to disinformation: Report of the independent High level Group on fake news and online disinformation*, Luxembourg, Publications Office of the European Union, 2018, pp. 5 et 10.

(313) COM (2018) 236, 26 avril 2018

(314) J. Balkin, « Free speech in the algorithmic society: big data, private governance, and new school speech regulation », *University of California Davis*, n° 51, 2018, pp. 1151 et s.

de fiabilité, les « signaleurs de confiance » ou, encore, les mesures de traçabilité des informations. La Commission préconise également, aux fins de garantir ou d'évaluer la véracité d'informations, la mise sur pied d'organes de *fast checking* indépendants et soumis à des règles d'éthique et de transparence rigoureuses, comme le Code de l'*International Fact-Checking Network*(315). Quatrièmement, la Commission prône la discussion entre l'ensemble des parties concernées par le problème de la désinformation(316), ce qui implique la participation des plateformes certes, mais également d'associations d'internautes ou de libertés civiles et d'autorités publiques, comme les autorités administratives en charge de l'audiovisuel ou de la protection des données.

13. Un *Code of Practice* léger avec droit de regard de la Commission. La réunion dite « *Multistakeholders* »(317), conviée par la Commission, ne réunissait pas tout ce beau monde mais bien certaines des plus importantes plateformes en ligne (Facebook, Google, Twitter, Mozilla et Microsoft(318)), les annonceurs ainsi que l'industrie publicitaire. Ces acteurs, sans attendre d'autres initiatives de la Commission, adoptent, en suivant la voie d'une autorégulation pure ou quasi pure, le *Code of Practice on Disinformation*. La Commission européenne n'aura d'autre choix que de l'approuver en septembre 2018(319). Le Code reprend certains engagements des parties signataires ou plutôt regroupe l'ensemble des différents engagements auxquels chaque partie pourra souscrire individuellement, partiellement ou non, et y répondre de manière originale et de bonne foi(320) : 1° transparence et analyse (*scrutiny*) des *ads* de manière à détecter l'origine des désinformations ; 2° identification de la publicité politique et de son sponsoring et diffusion d'opinions (*issue based advertising*) ;

(315) « *The International Fact-Checking Network is a unit of the Poynter Institute dedicated to bringing together fact-checkers worldwide. The IFCN was launched in September 2015 to support a booming crop of fact-checking initiatives by promoting best practices and exchanges in this field* ». Sur les compétences et le fonctionnement de ce réseau, voy. le site du réseau : https://www.poynter.org/ifcnfast-checking. On note que ce réseau a été à la base du réseau européen de « *fast-checking* » qui notamment a contrôlé la diffusion des informations lors des élections européennes et a répondu aux questions des citoyens. Lancé le 18 mars 2019, ce réseau baptisé « FactCheckEU » est un consortium de dix-neuf médias européens issus de treize pays différents (pour la France, « Les Observateurs » de France 24, « AFP Factuel » de l'AFP, « Fake off » de *20 Minutes*, « Les Décodeurs » du *Monde* et « CheckNews » de *Libération*).

(316) Rapport du High Level Group, *ibid*., pp. 7-8. À cet égard, la Commission prône les mesures de sensibilisation des internautes, l'éducation aux médias, ainsi que la mobilisation et la coopération de l'ensemble des *stakeholders* (pouvoirs publics, plateformes en ligne, annonceurs, signaleurs de confiance, journalistes et médias).

(317) « *The Multistakeholder Forum on Disinformation comprises two different and autonomous groups. On the one hand, major online platforms ad exchanges and their trade associations, the advertisers and agencies' associations and the European advertising self-regulatory body ("the Working Group"), and on the other hand representatives of the media, civil society, fact checkers and academia ("the Sounding Board")* ».

(318) Alors que les quatre premières sociétés étaient présentes à l'origine de l'adoption du Code en 2018, Microsoft a rejoint la liste des signataires en mai 2019.

(319) Commission européenne (DG Connect), « Code of Practice on Disinformation », 26 septembre 2018, mis à jour le 17 juin 2019, disponible sur https://ec.europa.eu/digital-single-market/en/news/code-practice-disinformation.

(320) « *The purpose of this Code is to identify the actions that Signatories could put in place in order to address the challenges related to "Disinformation"* ».

3° intégrité des services de manière à éviter des fausses représentations (*misrepresentations)* ou des spams ; 4° « *empowerment* » des consommateurs en privilégiant les messages authentiques, en développant des produits ou services indicateurs de la fiabilité des messages rencontrés sur la Toile en évitant des spams ou des *misrepresentations* et en donnant aux consommateurs l'accès à des sources alternatives et à des sites de dénonciation des messages de désinformation, éducation des internautes au jugement critique ; 5° aide au développement de la recherche, y compris académique, notamment pour la mise sur pied d'instruments d'intelligence artificielle d'analyse automatique des contenus (*content ranking algorithms*) et mise sur pied d'organes « indépendants » de *fast checking* et définition de procédures devant ces organes, politique de repérage des *chatbots* destinés à amplifier des messages de désinformation(321). En outre, les signataires s'engagent à publier un rapport sur les mesures prises à propos des différents objets, sur lesquels portent leurs devoirs. Ce rapport doit, de plus, reprendre certains indicateurs rendant transparentes l'importance du phénomène de désinformation, les plaintes soumises et les solutions apportées(322).

(321) « *The purpose of this Code is to identify the actions that Signatories could put in place in order to address the challenges related to "Disinformation" In line with the Commission's Communication, the Signatories of the Code of Practice recognise the importance of efforts to:*
(i) Include safeguards against Disinformation;
(ii) Improve the scrutiny of advertisement placements to reduce revenues of the purveyors of disinformation;
(iii) Ensure transparency about political and issue-based advertising, also with a view to enabling users to understand why they have been targeted by a given advertisement;
(iv) Implement and promote reasonable policies against misrepresentation;
(v) Intensify and demonstrate the effectiveness of efforts to close fake accounts and establish clear marking systems and rules for bots to ensure their activities cannot be confused with human interactions;
(vi) Intensify and communicate on the effectiveness of efforts to ensure the integrity of services with regards to accounts whose purpose and intent is to spread Disinformation, as per specifics assessed and determined by the Relevant Signatory, and consistently with Article 8 of the European Convention on Human Rights, the fundamental right of anonymity and pseudonymity, and the proportionality principle.
(vii) Consistently with Article 10 of the European Convention on Human Rights and the principle of freedom of opinion, invest in technological means to prioritize relevant, authentic, and accurate and authoritative information where appropriate in search, feeds, or other automatically ranked distribution channels. Be that as it may, Signatories should not be compelled by governments, nor should they adopt voluntary policies, to delete or prevent access to otherwise lawful content or messages solely on the basis that they are thought to be "false".
(viii) Ensure transparency with a view to enabling users to understand why they have been targeted by a given political or issue-based advertisement, also through indicators of the trustworthiness of content sources, media ownership and/or verified identity.
(ix) Dilute the visibility of disinformation by improving the findability of trustworthy content.
(x) Consider empowering users with tools enabling a customized and interactive online experience so as to facilitate content discovery and access to different news sources representing alternative viewpoints, also providing them with easily-accessible tools to report Disinformation.
(xi) Take the reasonable measures to enable privacy-compliant access to data for factchecking and research activities and to cooperate by providing relevant data on the functioning of their services including data for independent investigation by academic researchers and general information on algorithms ».
(322) « *Relevant Signatories commit to write an annual account of their work to counter Disinformation in the form of a publicly available report reviewable by a third party. The report may include details of any measures taken and the progress made by the Signatories to improve transparency regarding Disinformation…* ».

Face à cette initiative, la Commission européenne, sans doute prise de vitesse, approuve l'initiative purement privée mais exige que les rapports des signataires lui soient remis régulièrement. Le Code qualifie ce devoir des signataires d'engagement de coopération avec la Commission : « *The Signatories agree to cooperate with the European Commission in assessing the reporting on the functioning of the Code. This cooperation may include: Making available appropriate information upon request; Informing the Commission of the signature or withdrawal of any Signatories; responding to the Commission's questions and consultations; Discussing the abovementioned assessment and reports in meetings of the Signatories; and inviting the Commission to all such meetings* ». Un an après l'approbation du Code et la remise de différents rapports, certains progrès sont notés par la Commission(323), même si le dernier rapport rappelle la mauvaise coopération entre les chercheurs commissionnés par la Commission et les plateformes signataires. De manière générale, selon l'avis du « *Sounding Board* » indépendant mis en place par la Commission pour juger des progrès de la lutte contre la désinformation : « *the Code of Practice as presented by the working group contains no common approach-, no clear and meaningful commitments, no measurable objectives or KPIs, hence no monitor process, and no compliance or enforcement tool: it is by no means selfregulation, and therefore the Platforms, despite their efforts, have not delivered a code Practice* within *the accepted meaning of effective and accountable self-regulation* »(324).

14. Un retour de la réglementation législative ? Il ne peut être question ici de décrire toutes les initiatives législatives ni même d'approfondir celles retenues. Nous nous contenterons d'épingler trois initiatives : celle française, dont la portée est essentiellement la lutte contre la désinformation en période électorale, celle allemande au dispositif plus large(325) et celle en discussion au Royaume-Uni.

En France(326), fin décembre 2018, au terme de débats parlementaires houleux, les lois ordinaire et organique relatives « à la lutte contre la manipulation de l'information » ont finalement été adoptées(327). Leur contenu a trait à diverses obligations

(323) Voy. l'analyse par la Commission des rapports de mars (23 avril 2019, disponible à l'adresse : https://www.governmenteuropa.eu/code-of-practice-on-disinformation/93032/) : « *The Commission also welcomes the fact that the three signatories to the Code have taken action to scrutinize ads to exclude misrepresentation or spam. However, the quality of the information provided varies by platform. Furthermore, Facebook, Google and Twitter have all demonstrated progress in March to ensure the integrity of their services, which shows they take the fight against malicious bots and fake accounts seriously* ».

(324) Sounding Board, *Report*, 26 septembre 2018, disponible sur le site : ebu.ch/news/2018/09/sounding-board-of-forum-on-disinformation-online.

(325) Sur ces deux premières initiatives, lire les commentaires et les références de M. Hanot et A. Michel, « Entre menaces pour la société et risques réglementaires : les *Fake news*, un danger pour la démocratie », *op. cit.*,

(326) Pour un commentaire plus complet sur les lois françaises et la décision n° 2018-773 DC du 20 décembre 2018 rendue par le Conseil constitutionnel, L. Costes, « "*Fake news*" : publication de la loi relative à la lutte contre la manipulation de l'information », *RLDI*, n° 155, janvier 2019, pp. 32-33.

(327) Voy. loi organique française n° 2018-1201 du 22 décembre 2018 relative à la lutte contre la manipulation de l'information, *J.O.R.F.*, 23 décembre 2018 ; loi française n° 2018-1202 du 22 décembre 2018 relative à la lutte contre la manipulation de l'information, *J.O.R.F.*, 23 décembre 2018. Indiquons que le Conseil constitutionnel a validé ces lois avec certaines réserves. Sur une analyse de

imposées aux plateformes en ligne(328) dans le cadre du processus électoral. Ainsi, la loi exige des plateformes une information claire, loyale et transparente des utilisateurs à la fois sur l'identité des personnes physiques ou morales qui les rémunèrent afin de « promouvoir » certains contenus informationnels concourant au débat d'intérêt général (voire les montants reçus des sponsors pour la publication d'une telle information s'ils dépassent une certaine somme), mais également quant à l'utilisation de données à caractère personnel dans le cadre de la promotion de tels contenus. Aux fins de consignation de telles informations, un registre à accès public est mis sur pied. Les plateformes mettront à disposition des internautes un dispositif permettant à ces derniers d'alerter la plateforme en cas de fausses informations véhiculées par elle. Au-delà, la loi autorise les différents partis et groupements politiques, ainsi que toute personne ayant un intérêt à agir, à introduire une requête auprès du juge des référés pour que les hébergeurs, à défaut les fournisseurs d'accès internet, prennent les mesures proportionnées et nécessaires pour stopper la diffusion de « fausses informations ». On ajoute la promulgation de diverses mesures relatives, premièrement, à la promotion des contenus provenant des entreprises et agences de presse ; deuxièmement, à la lutte contre les comptes diffusant de fausses informations ; troisièmement, à l'éducation aux médias et, surtout, quatrièmement, nous y reviendrons (*infra*, n° 24), à la transparence des algorithmes utilisés et dans l'hypothèse où les plateformes utiliseraient des algorithmes pour référencer, classer ou recommander des contenus d'information participant au débat général, elles sont soumises à une obligation de publication de statistiques agrégées relatives au fonctionnement de ces algorithmes.

En Allemagne, le propos de la loi du 30 juin 2017 visant à améliorer l'application de dispositions existant sur Internet et, plus particulièrement, sur les réseaux sociaux (la « *NetzDG* »)(329) est plus large. Sont visés *ratione personae* les fournisseurs de services de médias de télécommunication « qui exploitent, dans un but lucratif, des plateformes sur Internet permettant à des utilisateurs d'échanger n'importe quel contenu avec d'autres utilisateurs, de le partager ou de le rendre accessible au

la décision n° 2018-773 DC du 20 décembre 2018 rendue par le Conseil constitutionnel à propos de la loi relative à la lutte contre la manipulation de l'information, voy. L. Costes, « "Fake news" : publication de la loi relative à la lutte contre la manipulation de l'information », *op. cit.*, pp. 32-33.

(328) Le législateur français, en l'article L111-7 du Code de la consommation français, définit comme suit l'« opérateur de plateforme en ligne » : « toute personne physique ou morale proposant, à titre professionnel, de manière rémunérée ou non, un service de communication au public en ligne reposant sur : 1° Le classement ou le référencement, au moyen d'algorithmes informatiques, de contenus, de biens ou de services proposés ou mis en ligne par des tiers ; 2° Ou la mise en relation de plusieurs parties en vue de la vente d'un bien, de la fourniture d'un service ou de l'échange ou du partage d'un contenu, d'un bien ou d'un service ».

(329) *Gesetz zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken (Netzwerkdurchsetzungsgesetz* – NetzDG), disponible sur : https://www.gesetze-im-internet.de/netzdg/NetzDG.pdf. Pour un commentaire en langue française très critique sur cette loi, lire B. Holznagel, « La *Loi d'application sur les réseaux* – L'approche allemande pour lutter contre les "fausses nouvelles", la violence et le discours terroriste dans les réseaux sociaux », in F. Sauvageau, S. Thibault et P. Trudel (dir.), *Les fausses nouvelles : nouveaux visages, nouveaux défis – Comment déterminer la valeur de l'information dans les sociétés démocratiques ?*, Laval, Presses de l'Université de Laval, 2018, pp. 197 et s.

public »[330]. *Ratione materiae*, la loi s'attaque à tout message à « contenu illicite » et renvoie, en ce qui concerne cette notion, à la définition du Code pénal allemand, soit tout message constituant une infraction depuis la formation d'organisation terroriste, la diffusion de pédopornographie, l'incitation à commettre une infraction violente majeure, la diffusion de représentations violentes, jusqu'à l'incitation à la haine, la falsification de données et de preuves, l'insulte ou encore la diffamation[331], les deux dernières infractions étant particulièrement appropriées pour lutter contre la désinformation. Il en découle que la diffusion de « fausses nouvelles » est susceptible de tomber sous le coup des infractions de diffamation ou encore de falsification de données et de preuves[332]. Le champ d'application précisé, retenons diverses obligations prescrites par la *NetzDG* aux plateformes visées par la loi[333] : la première vise la mise sur pied d'« une procédure efficace et transparent[e] facilement reconnaissable, directement accessible et disponible en permanence » pour les internautes[334] et la transparence due (rapport public semestriel) pour les plaintes reçues et le sort réservé à ces plaintes sont premièrement soumis, dans certaines circonstances, à une obligation de transparence par rapport aux plaintes reçues. On souligne qu'en cas de doute sur l'illicéité d'un message, la loi oblige au recours à un organe de « *Fast-checking* », désigné par la plateforme suivant des critères d'indépendance, de spécialité et de compétences fixés par la loi. En toute hypothèse, la plateforme doit informer sans délai l'auteur de la plainte de la solution prise et de sa motivation.

Le rapport final discuté à la House of Commons du Royaume-Uni : « *Disinformation and "fake news"* »[335] prolonge ces efforts en direction d'un retour vers la réglementation publique. L'annonce récente publiée par le gouvernement anglais

(330) Y compris des plateformes de musique, de ventes ou jeux en ligne, des réseaux sociaux professionnels, etc., mais à l'exception des « plateformes de contenu journalistique et rédactionnel », n'entrent pas dans la notion de « fournisseurs de services de médias de télécommunication ».

(331) NetzDG, § 1er, (3). Voy. B. Holznagel, « La *Loi d'application sur les réseaux* – L'approche allemande pour lutter contre les "fausses nouvelles", la violence et le discours terroriste dans les réseaux sociaux », *op. cit.*, pp. 204-205. Voy. égal. H. Tworek et P. Leerssen, « An analysis of Germany's NetzDG law », 15 avril 2019, p. 2, disponible sur https://www.ivir.nl/publicaties/download/NetzDG_Tworek_Leerssen_April_2019.pdf.

(332) L'infraction de diffamation est définie comme suit : le fait « d'affirmer ou de disséminer intentionnellement et en connaissance de cause un fait erroné sur autrui si ce fait est susceptible de le diffamer ou d'affecter négativement l'opinion publique à son endroit », B. Holznagel, « La *Loi d'application sur les réseaux* – L'approche allemande pour lutter contre les "fausses nouvelles", la violence et le discours terroriste dans les réseaux sociaux », *op. cit.*, en particulier la note 126, p. 205.

(333) Et ce, sous peine d'amendes administratives, pouvant atteindre des plafonds allant de 500 000 euros à 5 millions d'euros selon le type d'infraction et la gravité de la faute. À noter que, si l'infraction consiste dans le non-blocage ou la non-suppression d'une information réputée illicite, l'autorité administrative doit préalablement obtenir une décision judiciaire sur l'illicéité.

(334) La procédure est laissée au libre choix de la plateforme, mais la loi exige que la plateforme prenne immédiatement connaissance de la plainte soumise et qu'elle analyse l'éventuel caractère « illégal » du contenu litigieux ainsi que la nécessité de retrait ou de blocage en déans un délai de vingt-quatre heures pour les contenus manifestement illicites, de sept jours normalement et, en cas de doute, à l'issue de la procédure de *fast-checking*.

(335) House of Commons – Digital, Culture, Media and Sport Committee, *Disinformation and « fake news »: Final report*, 8th Report of session 2017-2019, HC 1791, publié le 18 février 2019.

de Boris Johnson de créer en 2020 un régulateur dédié pour contrôler les géants du numérique comme Google et Facebook fait largement écho à ce rapport. Si le projet est mené à son terme, le Royaume-Uni deviendrait l'un des premiers pays en Europe à se doter d'un régulateur spécifique pour la « *big tech* ». Le nouveau régulateur veillera au respect d'un code de bonnes pratiques et permettra un accès plus grand aux données pour les consommateurs. Le régulateur pourrait aussi délivrer des amendes supérieures à celles que prononce déjà la CMA (*Competition and Markets' Authority*), le gendarme des marchés du pays. Mais sa capacité réelle à réguler les GAFAM dépendra en grande partie de son budget et de ses équipes.

Le premier message du rapport est de souligner la responsabilité sociétale des plateformes tant de communication que d'accès à des contenus, identifiées comme une nouvelle catégorie d'entreprises de l'Internet. Cette responsabilité doit conduire à imposer une responsabilité juridique en ce qui concerne les contenus dommageables accessibles via ces plateformes. Le rapport en particulier dénonce le modèle d'affaires mis en place par ces plateformes, modèle centré sur l'optimisation des revenus publicitaires et qui contredit les exigences des droits de l'homme et en particulier de la vie privée(336). Par ailleurs, les enjeux démocratiques soulevés par la manipulation des opinions, y compris des votes des citoyens, requièrent une intervention de l'État. Ainsi, le rapport conclut, avec la commissaire à l'Autorité de protection des données (ICO)(337) : « *That is where we are right now and it is a very big job for both regulators and the policymakers to ensure that the right requirements oversight and sanctions are in place. There is an urgent need to establish independent regulation* ». Très concrètement, la House of Commons, qui approuve le rapport, estime qu'un code d'éthique développé par des experts et contrôlé par un régulateur public indépendant(338) doit être rendu obligatoire par la loi. Ce régulateur doit pouvoir exiger toute information des entreprises soumises à son autorité, accueillir les plaintes particulières des internautes, auditer les algorithmes

(336) À cet égard, l'analyse remarquable (pp. 40 et s.) des pratiques de Facebook sur la base des rapports et auditions de la FCC américaine et de l'ICO dans l'affaire *SIX4THREE* et *Cambridge Analytica*.

(337) Il s'agit de Mme E. Denham. L'ICO avait émis en septembre 2017 un excellent rapport sur les pratiques en particulier des GAFAM basées sur l'intelligence artificielle : *Big Data, artificial intelligence, machine learning and data protection*, ICO Publications, 4 septembre 2017.

(338) Le rapport (pp. 11 et s.) accorde une importance particulière à la mise sur pied par le Gouvernement en 2017 d'un *Centre for Data Ethics and Algorithms*, dont le rôle est de conseiller le gouvernement sur « *how to enable and ensure ethical, safe and innovative uses of data, including for AI* ». Nous reviendrons sur cet organe et le modèle qu'il représente dans la 3e partie (*infra*). Dans un autre rapport concomitant, cette fois émis par la *House of Lords* : *Regulating in a digital World* (2nd Report Session 2017-2019, publié le 9 mars 2019, H-L Paper 299), le Parlement britannique recommande la création d'un nouvel organe : « *the Digital Authority* », qui serait chargé de coordonner les activités des organes déjà en charge de la surveillance de l'Internet, ainsi OfCOM, ICO, CMA (sur les questions de concurrence jugées très importantes au regard des pratiques actuelles). Cette autorité aurait pour compétence à la fois d'évaluer les réglementations en vigueur au regard des progrès technologiques, de l'évolution des marchés et de l'impact sur la population, mais également d'adresser des recommandations au gouvernement et au Parlement.

utilisés par les entreprises. Au-delà, le rapport en appelle à une révision des lois électorales et, en particulier, de se protéger contre des manipulations électorales venant de pays tiers. Il plaide également pour un changement de la loi sur la protection des données qui devrait dorénavant également s'étendre aux données dérivées et surtout aux modèles qui président au fonctionnement des algorithmes. La promotion d'une politique coordonnée de « *Digital literacy* » (« *fourth pillar of education alongside reading, writing and maths* » !) et d'un journalisme de qualité est réclamée.

15. Les limites de l'autorégulation. L'analyse des législations ou des débats législatifs à laquelle nous venons de procéder témoigne de différentes vérités. La première s'énonce comme suit : qu'il s'agisse d'autorégulation ou de législation, on retrouve dans les mesures proposées de fortes similitudes : contrôles des *ads* ; transparence des sources des messages politiques ; attention aux systèmes technologiques en particulier d'intelligence artificielle mis en place pour détecter et bloquer les contenus dommageables ; mise en place de procédures de plainte et mise sur pied dans ce contexte d'organes de *fast-checking* ; promotion de sources d'information de qualité, insistance sur le rôle de l'éducation aux médias et de la recherche. La deuxième différencie les approches d'autorégulation et de réglementation publique : si les partisans du *Code of Practice* européen considèrent que la liberté d'entreprise doit permettre des autorégulations propres à chaque entreprise présentant des solutions variées et innovantes et, donc, en définitive au service du citoyen, qui décidera en toute transparence le choix de telle ou telle solution. Les tenants de l'intervention réglementaire dénient à ces acteurs leur légitimité à réguler seuls une activité dont l'enjeu est la démocratie. Sans doute, la loi française n'est-elle centrée que sur les questions de vote démocratique, seul objet de son intervention législative, mais déjà la loi allemande élargit la préoccupation en soulignant les dangers de manipulation des personnes que représentent les messages publicitaires comme d'opinions. Le rapport anglais va encore au-delà : il dénonce l'opacité des flux que cachent les systèmes d'informations et les *business models* mis en place par les plateformes. Il souligne les conséquences non seulement sur les individus, sur les processus démocratiques d'élection, mais également sur le marché de l'information, dont le fonctionnement s'éloigne du fonctionnement concurrentiel souhaitable.

Bref, la réglementation des plateformes de communication et d'informations, comme entreprises du numérique ayant un rôle particulier, s'impose. En premier lieu, elles constituent l'interface nécessaire, le « *gatekeeper* », pour l'exercice par chaque citoyen de deux services indispensables à tout citoyen dans la société de l'information et de la connaissance qui est la nôtre : celui de l'accès à l'information (les moteurs de recherche, les plateformes spécialisées en musique, en films, en photos…), et celui de la communication et de l'échange de messages. La réglementation imposée se déduit de ce service universel offert à tous et chacun et dont la qualité requiert une attention particulière au respect des personnes, de leur vie privée et de leur liberté, ce qui implique notamment la lutte contre la manipulation, y compris commerciale. Le second argument est plus économique : ces entreprises, précisément du fait de leur rôle de « *gatekeepers* », détiennent une puissance sur le marché de l'information

qui place toute autre entreprise et même l'autorité publique dans une situation de dépendance(339). Le rôle de l'État comme gendarme de la concurrence justifie également leur intervention réglementaire.

Ceci dit, il est intéressant de noter que cette intervention réglementaire a tout à gagner à laisser une place à la corégulation : il est clair que les solutions que les États souhaitent en termes de contrôle des *ads*, en termes de qualité des algorithmes d'intelligence artificielle qui contrôlent les contenus véhiculés ou rendus accessibles, en termes de procédures de plainte et de mode des solutions des litiges, en termes de politique de promotion des contenus de qualité, etc., dépendront dans leur mise en œuvre concrète des orientations et actions innovantes et originales de chacune des plateformes. Bref, la réglementation publique a tout à gagner à être moins-disante, proportionnée et limitée à ce qui est nécessaire pour l'obtention des finalités décrites ci-dessus, en d'autres termes, à poser les balises et à renvoyer pour le reste à l'action et aux solutions, qui seront élaborées par les acteurs privés.

Il s'agit bien d'une délégation aux acteurs privés, délégation sans doute sous contrôle des autorités publiques ou plutôt d'un organe « *multistakeholders* », indépendant. Une corégulation semble être la voie à suivre en matière de désinformation. Les balises posées par les textes réglementaires nous semblent devoir être minimales, à l'inverse de celles très (trop) nombreuses inscrites dans les législations de protection des données. La différence se justifie. Alors qu'il s'agissait avec le RGPD d'une législation positive au service des libertés, il s'agit ici de veiller à ne toucher à la liberté d'expression et d'information que dans la stricte mesure où l'intérêt général et l'intérêt d'autrui l'emportent et, par là, de contrôler les filtres que les *gatekeepers* pourraient instaurer au nom de valeurs et d'intérêts privés, véritable censure privée plus insidieuse et plus multiforme que celle que l'État pourrait mettre en place.

Section 3.
La technologie comme mode de régulation ?

16. La technologie, un mode d'effectivité de la régulation… (trop) efficace ? Les législateurs du numérique ont pris l'habitude de se référer à la technologie pour rendre plus effectives les dispositions légales. On peut concevoir – et l'exemple du *Code of Practice on Disinformation* le montre à souhait – que l'autorégulation trouve également dans l'implémentation de systèmes technologiques une plus-value

(339) À cet égard, de manière significative, les réflexions adressées par le rapport britannique à propos des cessions et/ou partages de données occultes via la « *Private Extended API Addendum* » entre Facebook, Spotify, Tax App, AirBnB révélés par les enquêtes de la *Federal Trade Commission* (FTC) américaine (pp. 28 et s.). « *Private Extended APIs' means a set of APIs and services provided by Facebook to Developer that enables Developer to retrieve data or functionality related to Facebook that is not generally available under platform, which may include persistent authentication, photo upload, video upload, messaging and phonebook connectivity* ».

à son effectivité. La technologie est sans doute le moyen le plus efficace pour garantir l'implémentation des dispositions des régulations, qu'elles soient législatives ou d'autorégulation : on pourrait parler de « *Privacy Enhancing Technologies* » (PET), de « *Consumer Protection Enhancing Technologies* » (CEPT), de « *Intellectual Property Enhancing Technologies* » (IPPET) et de « *Content Control Enghancing Technologies* » (CCET)(340). Prenons quelques exemples : ainsi, à l'appui du souci de protection des consommateurs, une disposition des conditions générales contractuelles, particulièrement importante pour le consommateur, apparaîtra en surbrillance, voire fera l'objet d'un pop-up et nécessitera un : « J'accepte » séparé avant la signature de l'accord global. Le blocage, le déférencement ou la déclassification automatique d'un message illicite ou contraire au code de conduite auquel le site web souscrit (par exemple, contrôle de la violence des images ou suppression de messages incorrects) sont d'autres exemples technologiques de mise en œuvre, cette fois en matière de contrôle de contenus. La technologie permet l'intervention automatique sur la base d'un programme dont les paramètres sont dictés, on l'espère, en conformité avec la régulation, qu'elle soit privée ou publique. On peut ainsi multiplier les exemples.

17. « *Code makes law more effective*… ». Le titre choisi paraphrase la phrase célèbre de Lessig, tout en la corrigeant quelque peu : nous pensons que, dans la plupart des cas, c'est-à-dire sauf exception (nous reviendrons en particulier sur la problématique de l'IA et du *deep learning*, *infra*, n^{os} 21 et s.), la technologie ne constitue pas en principe la « loi » : elle se contente, dans la plupart des cas, de relayer la régulation privée ou publique pour la rendre plus effective. Si le rôle de la technologie dans l'*enforcement* des régulations privées est évident (*infra*, n° 20), il importe également de montrer combien, dans des textes récents relatifs à la société du numérique, le législateur s'est appuyé sur la technologie pour rendre plus effectives ses dispositions. Sans vouloir être exhaustif loin de là, nous nous limiterons à évoquer deux exemples(341) parmi les plus remarquables : le RGPD et la directive sur le droit d'auteur.

En ce qui concerne le premier texte, on citera d'abord les principes dits de « *privacy by design* » et de « *privacy by default* » pour illustrer notre propos. À propos du « *privacy by design* », l'article 25.1 du RGPD énonce : « Compte tenu de l'état des connaissances, des coûts de mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques, dont le degré de probabilité et de gravité varie, que présente le traitement pour les droits et libertés des personnes physiques, le responsable du traitement met en œuvre, tant au moment de

(340) Ce sont les acronymes que je proposais dès 2004, à propos des liens entre droit et technologie : Y. Poullet, « Technology and law: from alliance to challenges », in U. Gasser (ed.), *Information Quality Regulation: Foundations, Perspectives and Applications*, Baden-Baden, 2004.

(341) D'autres exemples peuvent être tirés de la transposition et la mise en œuvre de la directive sur l'e-commerce du 8 juin 2000 ou de la directive relative à la protection des consommateurs dans le cadre des contrats à distance, de la décision-cadre 2008/913/JAI sur la lutte contre certaines formes et manifestations de racisme et de xénophobie au moyen du droit pénal mise en œuvre notamment via un code de conduite, signée par les principales plateformes privées et qui a fait l'objet d'une évaluation en 2016 : European Commission, *Fighting Illegal Online Hate Speech: First Assessment of the New Code of Conduct*, Press Release, 6 décembre 2016, http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50840.

la détermination des moyens du traitement qu'au moment du traitement lui-même, des mesures techniques et organisationnelles appropriées ». Ce principe énoncé il y a plus de dix ans(342) est affirmé par le RGPD et, très récemment, l'EDPB lui a consacré des « lignes directrices »(343) qui amplifient encore la portée de celui-ci. La technologie doit être au service des libertés, et les choix d'infrastructure et de logiciels opérés par les responsables de traitement dès la conception du système et à tous les stades de son développement et de son évolution, insistent le texte et les lignes directrices, doivent répondre autant que possible aux prescrits du Règlement et assurer la sécurité des traitements, que l'on pense aux techniques de pseudonymisation, de cryptographie, aux technologies de contrôle d'accès, au floutage des visages, aux restrictions de circulation des données inscrites dans les messages eux-mêmes, etc.(344). Le règlement plaide de manière claire pour un « *value-sensitive design* » de nos systèmes d'information(345). La technologie, les infrastructures mises en place, les produits offerts, les applications intégrées doivent toujours être évalués du point de vue des risques que la technologie fait courir au développement de nos libertés et au respect de notre dignité. On ajoute que le RGPD réclame (art. 32 et s.) du responsable des mesures techniques de sécurité : « Compte tenu de l'état des connaissances, des coûts de mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques, dont le degré de probabilité et de gravité varie, pour les droits et

(342) « Le concept de la "protection de la vie privée dès la conception" (*privacy by design*) a été développé à l'initiative de la préposée à la protection des données de l'État d'Ontario au Canada, Ann Cavoukian (voy. *Operationalizing Privacy by Design: A Guide to Implementing Strong Privacy Practices*, Toronto, 2012) : chaque nouvelle technologie traitant des données personnelles ou permettant d'en traiter doit garantir dès sa conception et lors de chaque utilisation, même si elle n'a pas été prévue à l'origine, le plus haut niveau possible de protection des données. Cette idée a notamment été plébiscitée par une résolution de la 32e conférence internationale des préposés à la protection des données les 27-29 octobre 2010, qui recommande aux États d'intégrer ce concept à leur législation » (J.C. Schwaab : http://www.schwaab.ch/archives/2013/09/26/privacy-by-design-by-default-inverser-la-logique-de-protection-des-donnees-en-faveur-des-utilisateurs/).

(343) EDPB, *Guidelines 4/2019 on Article 25: data Protection by design and by default*, 13 novembre 2019.

(344) Les lignes directrices reprennent point par point les différents principes du RGPD (transparence, légitimité, loyauté, détermination des finalités, minimisation des données, durée limitée de conversation, sécurité) et, pour chacun, décrivent les « *Key design and default elements* » à prendre en considération : ainsi, pour la transparence, les éléments cités sont : « *clarity, semantics, accessibility, contextual, relevance, universal design, comprehensible, muti-channel* ». Le texte est accompagné d'exemples très utiles. Il est intéressant de noter que les lignes directrices en appellent à une responsabilité non seulement des responsables, mais également des « *technology providers* » et des certificateurs.

(345) À cet égard, lire les nombreuses réflexions et références proposées par L. Costa (*Virtuality and Capabilities in a World of Ambient Intelligence*, Law, Governance and Technology Series, vol. 32, Springer Books, 2016, n° 180) : « *Underlining the ethical relevance of design, Oosterlaken points that both "values" – such as privacy, autonomy sustainability and justice – and their opposites can be realized through technology. This ethical relevance is at the roots of the "value-sensitive design" research field which, departing from traditional approaches to design – based on values such as functionality and reliability and focused on comfort and pleasure – advances that design shall take these values into account In a parallel to the shift from "traditional" to "value-sensitive" design, Oosterlaken proposes the shift from "traditional" to "capability-sensitive" design: technology not being neutral, its design must take in consideration how technology will impact on persons' capabilities* ».

libertés des personnes physiques, le responsable du traitement et le sous-traitant sont tenus [de mettre] en oeuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque… », et l'article 35 exige, en cas de traitement à haut risque, une évaluation des différentes solutions technologiques afin de minimiser les risques courus par les personnes concernées(346).

La révision récente de la directive sur le droit d'auteur dans la société de l'information est intéressante. On sait que la directive de base(347) non seulement consacrait la protection des œuvres par des mesures technologiques (*Digital Rights Management Systems, Watermarking…*), mais, en outre, protégeait ces mesures contre tout contournement. La justification était simple : le droit d'auteur trouvait dans l'implémentation de telles mesures techniques une protection bien plus efficace aux œuvres et à leurs auteurs ou ayant droit les mesures techniques permettent en effet le plus souvent une protection *a priori* de l'oeuvre, là où le recours aux tribunaux ne peut s'exercer qu'*a posteriori*, c'est à dire après constatation d'une violation des droits sur l'oeuvre ? Le considérant 47 doit être cité à cet égard : « L'évolution technologique permettra aux titulaires de droits de recourir à des mesures techniques destinées à empêcher ou à limiter les actes non autorisés par les titulaires d'un droit d'auteur, de droits voisins ou du droit *sui generis* sur une base de données. Le risque existe, toutefois, de voir se développer des activités illicites visant à permettre ou à faciliter le contournement de la protection technique fournie par ces mesures. Afin d'éviter des approches juridiques fragmentées susceptibles d'entraver le fonctionnement du marché intérieur, il est nécessaire de prévoir une protection juridique harmonisée contre le contournement des mesures techniques efficaces et contre le recours à des dispositifs et à des produits ou services à cet effet ». Si on y regarde de près, on note que l'efficacité de ces mesures donne insidieusement à des œuvres numérisées une protection bien au-delà de celle inscrite au cœur des législations qui ont reconnu ce droit. Ainsi, ces mesures mettent à mal la parodie, la citation et les intérêts reconnus légitimes comme l'enseignement ou la recherche, elles dénoncent toute découverte de similarités, même inconscientes, même partielles, d'une œuvre, reconnaissant ainsi à chaque partie la qualité du tout. Elles renversent la charge de la preuve, intervenant *a priori*, et non plus *a posteriori*. Enfin, elles pourraient protéger une œuvre ne méritant pas la protection du droit d'auteur. L'effectivité technologique peut-elle ainsi remettre en cause les équilibres souhaités et inscrits au cœur des législations ? En d'autres termes, pour reprendre les trois critères d'analyse de l'autorégulation, la protection induite par

(346) Le lien entre l'article 25 et les articles relatifs à la sécurité et à l'évaluation des risques est longuement explicité dans les lignes directrices du 13 novembre 2019 de l'EDPB. « *The GDPR adopts a coherent risk based approach throughout its provisions, in Articles 24, 25, 32 and 35 with a view to identify appropriate technical and organizational measures to protect individuals, their personal data and comply with the requirements of the GDPR The risk and the assessment criteria are the same…* » (p. 9).

(347) Directive 2001/29/CE du Parlement européen et du Conseil du 22 mai 2001 sur l'harmonisation de certains aspects du droit d'auteur et des droits voisins dans la société de l'information, *J.O.*, L 167 du 22 juin 2001, pp. 0010-0019.

la technologie peut-elle être non conforme à la loi et imposer sa régulation propre, conformément à l'affirmation de Lessig[348] : « *Code is Law* » ?

Le texte nouveau qui modifie sur certains points la directive de 2001, intitulé « Le droit d'auteur dans le marché unique numérique »[349], est intéressant dans la mesure où, premièrement, il accroît le recours aux mesures technologiques, réclamant indirectement aux plateformes de mises en ligne de prévoir des systèmes d'intelligence artificielle, capables de détecter toute copie, mais, secondement, dans le même temps, le texte demande que soient respectées, dans la mise en place de ces systèmes de détection et de blocage, les exceptions prévues par le droit d'auteur. Détaillons ces deux points. Le texte renforce la légitimité de la délégation aux mesures technologiques en particulier même si elles ne sont pas nommées, celles recourant à l'intelligence artificielle. L'article 17 de cette directive impose en effet aux « fournisseurs de services de partage de contenus en ligne » (en d'autres termes, les plateformes de communication et d'informations), selon les termes du considérant 66, « de fournir leurs meilleurs efforts, conformément aux normes élevées du secteur en matière de diligence professionnelle, pour éviter que des œuvres et autres objets protégés non autorisés, tels qu'ils sont identifiés par les titulaires de droits concernés, ne soient disponibles sur leurs services. À cette fin, les titulaires de droits devraient fournir les informations pertinentes et nécessaires aux fournisseurs de services en tenant compte, entre autres facteurs, de la taille des titulaires de droits et de leurs types d'œuvres et autres objets protégés ». Ce devoir de prendre des mesures ne vise pas nécessairement des mesures techniques, affirme certes la Commission[350], mais on voit mal comment des fournisseurs de services de partage de contenus en ligne de taille importante, comme Facebook, Spotify, Google… pourront faire preuve de leurs efforts raisonnables de filtrer les contenus illicites, sans recourir à des moyens

(348) « Une idée définit la pensée de la première génération au sujet de cet espace. Le cyberespace, disait-on, ne peut pas être régulé. Il ne "peut pas être gouverné", il a une habileté innée à résister à la régulation. C'est là sa nature, son essence, c'est ainsi que sont les choses […]. Le cyberespace est un espace de non-contrôle », L. Lessig, *Code and other Laws of Cyberespace*, New York, Basic Books, 1999, p. 24 ; comp. N. Negroponte, *Being Digital*, New York, Vintage Books, 1995, p. 237 : « [Le droit est] un poisson mourant sur les quais, parcouru de spasmes, tentant de happer une dernière bouffée d'air, en vain, car le monde numérique est un lieu différent ». Sur l'affirmation prêtée à Lessig, plus que tenue par lui, lire notamment P. Mathias, « From Code to Law », in F. Massit-Follea, C.L. Meadel et L. Monnoyer (eds), *Normative Experience in Internet Politics*, Presse des Mines, 2012, pp. 24 et s.

(349) Directive (UE) 2019/790 du Parlement européen et du Conseil du 17 avril 2019 sur le droit d'auteur et les droits voisins dans le marché unique numérique et modifiant les directives 96/9/CE et 2001/29/CE (texte présentant de l'intérêt pour l'EEE), PE/51/2019/REV/1, *J.O.*, L 130 du 17 mai 2019, pp. 92-125.

(350) Sur ce point, la Commission européenne a été très claire dans sa fiche d'information publiée le 26 mars 2019 : « Les nouvelles règles n'imposent pas d'utiliser des filtres de téléchargement. Elles n'imposent pas non plus aux plateformes de mise en ligne de contenus par les utilisateurs d'appliquer une technologie spécifique de reconnaissance des contenus illicites. En vertu des nouvelles règles, certaines plateformes en ligne seront tenues de conclure des accords de licence avec les titulaires de droits – par exemple, des producteurs de musique ou de films – pour pouvoir utiliser des œuvres musicales, des vidéos ou d'autres contenus protégés par le droit d'auteur. En l'absence d'accords de licence, ces plateformes devront faire tout leur possible pour s'assurer que les contenus non autorisés par les titulaires de droits ne sont pas disponibles sur leur site web. L'obligation de "faire tout son possible" n'impose aucun moyen ni aucune technologie spécifique ».

technologiques. Le second point est d'exiger que les mesures techniques retenues de protection des œuvres, dont notamment mais pas uniquement celles de l'article 17, soient conformes au droit. Le considérant 7 de la directive de 2019 est clair : « La protection des mesures technologiques prévue dans la directive 2001/29/CE reste indispensable pour assurer la protection et l'exercice effectif des droits conférés aux auteurs et aux autres titulaires de droits en vertu du droit de l'Union. Il convient de maintenir cette protection, tout en veillant à ce que l'utilisation de mesures technologiques n'empêche pas les bénéficiaires de jouir des exceptions et limitations prévues par la présente directive ». Ce principe général de conformité des solutions technologiques aux dispositions légales est souligné amplement à propos des mesures qui seraient prises en vertu de l'article 17 : « Les mesures prises par les fournisseurs de services de partage de contenus en ligne en coopération avec les titulaires de droits ne devraient pas avoir pour conséquence d'empêcher la disponibilité de contenus qui ne portent pas atteinte au droit d'auteur, y compris d'œuvres ou d'autres objets protégés dont l'utilisation est couverte par un accord de licence, ou par une exception ou une limitation au droit d'auteur ou aux droits voisins. Les mesures prises par ces fournisseurs de services ne devraient, dès lors, pas affecter les utilisateurs qui utilisent les services de partage de contenus en ligne afin de téléverser de manière licite des informations sur ces services et d'y accéder de manière licite »(351). Il s'agit d'affirmer le rôle de la technologie, mais de rappeler que les balises de son intervention sont bien fixées par la loi.

18. Assurer l'effectivité de l'autorégulation et de la corégulation. Les exemples ne manquent pas et sans doute posent nombre de questions lorsque la technologie permet à une autorégulation occulte la possibilité d'être pleinement efficace(352). L'exemple des systèmes automatisés de *rankings* des moteurs de recherche privilégiant les sites « amis » de la plateforme peut être cité. Elle a donné lieu à des dispositions de la loi française « pour une République numérique »(353) qui

(351) Cons. 66. Le texte de l'article 17.7 transcrit ce principe : « La coopération entre les fournisseurs de services de partage de contenus en ligne et les titulaires de droits ne conduit pas à empêcher la mise à disposition d'œuvres ou d'autres objets protégés téléversés par des utilisateurs, qui ne portent pas atteinte au droit d'auteur et aux droits voisins, y compris lorsque ces œuvres ou autres objets protégés sont couverts par une exception ou une limitation. Les États membres veillent à ce que les utilisateurs dans chaque État membre puissent se prévaloir de l'une quelconque des exceptions ou limitations existantes suivantes lors du téléversement et de la mise à disposition de contenus générés par les utilisateurs sur les services de partage de contenus en ligne : a) citation, critique, revue ; b) utilisation à des fins de caricature, de parodie ou de pastiche ».

(352) S. Barocas, S. Hood et M. Ziewitz, « Governing algorithms: a provocation piece », 2013, disponible à l'adresse : https://ssrn.com/abstract=2245322.

(353) Pris en application de la loi pour une République numérique n° 2016-1321 du 7 octobre 2016, ces décrets sont le fruit d'une large concertation au sein du Conseil national de la consommation (CNC) ainsi qu'avec les représentants des entreprises des secteurs concernés. Ces trois décrets doivent permettre de renforcer les obligations de transparence et de loyauté que doivent respecter les plateformes numériques. Finalement, les consommateurs pourront accéder à des informations plus claires, objectives et transparentes : les plateformes qui valorisent des contenus, des biens ou des services proposés par des tiers, tels que les moteurs de recherche, réseaux sociaux ou comparateurs, devront préciser les critères de référencement et de classement qu'elles utilisent ; les sites publiant des avis de consommateurs devront préciser s'ils ont été vérifiés et selon quelle méthodologie ; les places de marchés et sites d'économie collaborative devront fournir des informations essentielles qui peuvent

impose (art. 49 et s.) des obligations de transparence et de loyauté aux opérateurs de plateformes en ligne(354). Limité aux relations B2B(355), le règlement européen récent impose de même aux plateformes d'information et de communication des obligations de transparence et interdise certaines pratiques de manière à combattre une telle autorégulation contraire aux règles d'une concurrence loyale et honnête. On sait, de même, que le choix des publicités affichées par les sites web, les messages privilégiés par les plateformes de discussion sont réglés par des algorithmes d'intelligence artificielle qui sont dictés partiellement, du moins par les opérateurs des réseaux(356).

orienter les choix des consommateurs : la qualité du vendeur, le montant des frais de mise en relation facturés par la plateforme, l'existence d'un droit de rétraction, l'existence d'une garantie légale de conformité ou encore les modalités de règlement des litiges ; les plateformes les plus visitées, c'est-à-dire celles dont le nombre de connexions mensuelles est supérieur à 5 millions de visiteurs uniques, seront tenues de suivre des bonnes pratiques en matière de clarté, de transparence et de loyauté, qui devront être consultables en ligne.

(354) Art. 49 de la loi : « I. Est qualifiée d'opérateur de plateforme en ligne toute personne physique ou morale proposant, à titre professionnel, de manière rémunérée ou non, un service de communication au public en ligne reposant sur : 1° Le classement ou le référencement, au moyen d'algorithmes informatiques, de contenus, de biens ou de services proposés ou mis en ligne par des tiers ; 2° Ou la mise en relation de plusieurs parties en vue de la vente d'un bien, de la fourniture d'un service ou de l'échange ou du partage d'un contenu, d'un bien ou d'un service. II. – Tout opérateur de plateforme en ligne est tenu de délivrer au consommateur une information loyale, claire et transparente sur : 1° Les conditions générales d'utilisation du service d'intermédiation qu'il propose et sur les modalités de référencement, de classement et de déréférencement des contenus, des biens ou des services auxquels ce service permet d'accéder ; 2° L'existence d'une relation contractuelle, d'un lien capitalistique ou d'une rémunération à son profit, dès lors qu'ils influencent le classement ou le référencement des contenus, des biens ou des services proposés ou mis en ligne ; 3° La qualité de l'annonceur et les droits et obligations des parties en matière civile et fiscale, lorsque des consommateurs sont mis en relation avec des professionnels ou des non-professionnels ».

(355) Règlement (UE) n° 2019/1150 du Parlement européen et du Conseil du 20 juin 2019 promouvant l'équité et la transparence pour les entreprises utilisatrices de services d'intermédiation en ligne, *J.O.*, L 186 du 11 juillet 2019, pp. 57 et s. : « Le classement des biens et services par les fournisseurs de services d'intermédiation en ligne a une incidence importante sur le choix des consommateurs et, par conséquent, sur la réussite commerciale des entreprises utilisatrices offrant ces biens et services aux consommateurs. Le classement rend compte de la priorité relative accordée aux offres des entreprises utilisatrices ou de la pertinence donnée aux résultats de recherche, tels qu'ils sont présentés, organisés ou communiqués par les fournisseurs de services d'intermédiation en ligne ou les fournisseurs de moteurs de recherche en ligne, résultant de l'utilisation du séquençage algorithmique, de mécanismes d'évaluation ou de notation, de la mise en surbrillance, d'autres outils de mise en évidence ou d'une combinaison de ces différents moyens ».

(356) Ceci ne va pas jusqu'à rendre responsable un moteur de recherche des résultats de la recherche et en particulier des conséquences qu'un internaute pourrait tirer de la juxtaposition de sites. On cite à cet égard l'attendu de la Cour de cassation française du 19 juin 2013 (arrêt n° 625) dans une affaire où le moteur de recherche de Google avait rapproché à partir des mots-clés d'interrogation deux sites qui accréditaient une image négative du plaignant. « La fonctionnalité aboutissant au rapprochement critiqué est le fruit d'un processus purement automatique dans son fonctionnement et aléatoire dans ses résultats, de sorte que l'affichage des "mots-clés" qui en résulte est exclusif de toute volonté de l'exploitant du moteur de recherche d'émettre les propos en cause ou de leur conférer une signification autonome au-delà de leur simple juxtaposition et de leur seule fonction d'aider à la recherche ».

Le cas déjà discuté du *Code of Practice on Disinformation* illustre une hypothèse d'autorégulation largement publiée. Ici également, les références à la technologie sont nombreuses. Ainsi, la disposition « *Scrutiny of ad placements* » mentionne explicitement : « *such policies will include the use of brand safety and verification tools* ». Et l'annexe 2 mentionne les mesures bien souvent technologiques prises par les différents signataires en ce qui concerne l'implémentation des différentes dispositions du *Code of Practice*.

19. L'IA comme technologie particulière au service de la régulation. Que l'IA, comme technologie particulière et, pour être plus précis, les systèmes auto-apprenants dits de « *machine learning* », voire mieux de « *deep learning* »[(357)], offrent à la régulation des instruments encore plus puissants que les technologies habituelles pour vérifier leur respect, voire prendre des décisions d'exécution de ces régulations, est indiscutable. Pour nombre de pouvoirs, tant publics que privés, l'IA est devenue l'outil indispensable de définition des stratégies d'actions, tant elle permet d'optimiser les choix, et ce, à partir d'éléments divers et variés, tant internes qu'externes, c'est-à-dire en provenance du contexte environnemental dans lequel ces stratégies doivent se déployer. Au-delà de la définition de la stratégie, ces instruments permettront de définir les paramètres à prendre en compte pour la définition de la régulation *ad hoc*, voire autoriseront la mise en place de systèmes automatisés de mise en œuvre de la réglementation. Ainsi, si on pense aux pouvoirs publics, définir la politique des logements sociaux, une réglementation appropriée sur les conditions d'octroi de tels logements, mais également *in fine* la mise en œuvre de cette politique par la vérification automatique des conditions d'octroi des logements, est permis grâce à des outils, qu'il s'agisse de systèmes dits

(357) L'intelligence artificielle est définie par le Larousse comme « l'ensemble des théories et des techniques mises en œuvre en vue de réaliser des machines capables de simuler l'intelligence ». Sur les définitions des notions de « *machine learning* » et de « *deep learning* », lire notamment A. Renda, *Artificial intelligence – Ethics, Governance and Policy Challenges*, Report of a CEPS Task Force, CEPS, Brussels, février 2019 ; Y. Poullet et B. Frenay, *Rapport et propositions de recommandations sur le « Profilage et la Convention 108+ du Conseil de l'Europe »*, Strasbourg, Conseil de l'Europe, novembre 2019, Comité consultatif de la Convention n° 108 pour la protection des personnes, disponible à l'adresse : www.crid.be/pdf/public/8504.pdf. Ce rapport proposait les définitions suivantes : « a. intelligence artificielle : théories et techniques dont le but est de reproduire par une machine des capacités cognitives d'un être humain. Les développements actuels visent, par exemple, à pouvoir confier à une machine des tâches complexes auparavant déléguées à un humain ; b. L'expression "traitement utilisant des procédés d'apprentissage automatique" (*machine learning*) signifie un traitement utilisant des méthodes particulières d'intelligence artificielle qui se fonde sur des approches statistiques pour donner aux ordinateurs la capacité d'"apprendre" à partir de données, c'est-à-dire d'améliorer leurs performances à résoudre des tâches sans être explicitement programmés pour chacune ; c. L'expression "apprentissage profond" (*deep learning*) signifie un ensemble de méthodes d'apprentissage automatique tentant de modéliser avec un haut niveau d'abstraction des données grâce à des architectures articulées de différentes transformations non linéaires ; d. Le terme "mégadonnées" (*big data*) désigne des ensembles de données extrêmement volumineux et hétérogènes, qui peuvent être analysés par ordinateur en vue d'en extraire des inférences statistiques sur les schémas, les tendances et les corrélations de données ».

experts ou de *machine learning.* Ainsi, si on pense aux pouvoirs privés, mettre au point une politique de profilage qui maximise les revenus d'une entreprise et, en fonction de cela, traduire cette politique en des algorithmes qui, dans le cadre d'un système de *deep learning*, permettront d'afficher suivant les règles définies au préalable, la publicité, voire le prix le plus adéquat, est désormais possible.

20. Les applications de l'IA en droit et leurs risques. L'intelligence artificielle se caractérise par la possibilité de travailler sur de vastes bases de données (*big data*) *:* du texte, des sons, des images de provenance et de nature diverses : l'Internet des objets, la géolocalisation, les habitudes de *surfing*, des scanners constituent autant de sources de données exploitables par les systèmes d'IA. Ses algorithmes se nourrissent des corrélations qu'elles peuvent établir statistiquement entre ces données au fur et à mesure de leur collecte, de leur stockage et de leurs traitements, qui peuvent être localisés en des endroits différents (*edge computing).*

Quelques caractéristiques des systèmes d'IA peuvent être épinglées.

• Les applications de l'IA conduisent à un renversement de paradigme dans le fonctionnement des systèmes informatiques(358). Traditionnellement, un programmeur travaille sur la base de règles appliquées à des données. Dans le *machine learning*, le principe est, au contraire, de tirer des données et des résultats d'actions collectées (par exemple, M. X qui a surfé sur telle page, telle page de tel site, qui s'est déplacé de tel à tel endroit de telle manière, qui a tel type de conduite de son véhicule, qui a écouté les plages musicales suivantes avec tel volume sonore… est intéressé par un voyage aux Bahamas), pour les agréger avec des données relatives à des millions d'autres personnes connectées et en déduire une règle : M. X doit être intéressé par une publicité relative à un séjour à Londres. On retient que la règle (ou plutôt le modèle(359)) n'est pas causale, mais est inférée par de pures corrélations entre données ; qu'elle n'est pas non plus stable et qu'elle peut difficilement s'exprimer vu la complexité des liens entre les données établis par les diverses couches de réseaux de neurones qui constituent le système d'IA.

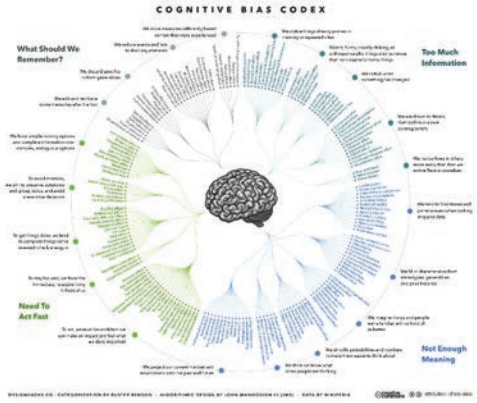
Ce mode de fonctionnement explique les risques liés au fonctionnement des systèmes d'IA. L'algorithme peut présenter des erreurs soit dans sa conception, soit dans les données reprises, fausses ou de mauvaise qualité, soit dans son adéquation au problème à résoudre. Pire, les données ou les algorithmes choisis peuvent contenir

(358) Joint Research Centre (JRC), *Artificial Intelligence: A European Perspective, A Flagship Report from the EU JRC*, EU Publications, 2018, pp. 7-8.

(359) Notre rapport, cité note 357, proposait la définition suivante : « Le terme "modèle" est une abstraction mathématique utilisée dans les méthodes d'apprentissage automatique, qui fournit une description simplifiée des données pour résoudre la tâche à effectuer ».

certains biais(360) qui faussent les résultats ou ont pour conséquence de discriminer certaines personnes(361) ou parfois certains groupes. Enfin, l'introduction malicieuse de quelques données, par exemple, quelques pixels dans un système d'IA de reconnaissance faciale, peut conduire à des erreurs ou non-sens des résultats obtenus. Comme le note le Groupe d'experts indépendants de haut niveau sur l'intelligence artificielle(362), les risques sont bien plus larges que les seuls risques individuels, ils sont également collectifs(363) : « *AI systems should not harm human beings. By design, AI systems should protect the dignity, integrity, liberty, privacy, safety, and security of human beings in society and at work. AI systems should not threaten the democratic process, freedom of expression, freedoms of identify, or the possibility to refuse AI services. At the very least, AI systems should not be designed in a way that enhances existing harms or creates new harms for individuals. Harms can be physical, psychological, financial or social. AI specific harms may stem from the treatment of data on individuals (i.e. how it is collected, stored, used, etc.). To avoid harm, data collected and used for training of AI algorithms must be done in a way that avoids discrimination, manipulation, or negative profiling. Of equal importance, AI systems should be*

(360) Voilà la façon dont Wikipédia présente les risques de biais.



(361) Ainsi, l'analyse par un système d'IA des quartiers susceptibles de favoriser une population criminogène met en cause non seulement, à titre de personnes, les personnes physiques de ce quartier, mais également le quartier comme tel, son image, et entraînant des conséquences sociales (personnes désertant le quartier ou refusant de s'y installer), voire la surveillance accrue de la police. Il s'agit donc d'un risque Ce risque de discrimination est d'autant plus important que le fonctionnement du mécanisme décisionnel apparaît comme neutre et objectif et que l'opacité de son fonctionnement empêche le décodage de la soi-disant « logique » suivie.

(362) High Level Expert Group on Artificial Intelligence, *Lignes directrices en matière d'éthique pour une IA digne de confiance*, Commission européenne, 10 avril 2019.

(363) Sur ce point, lire les lignes directrices du Conseil de l'Europe à propos des mégadonnées, du 23 janvier 2017, qui n'hésitent pas à l'affirmer explicitement : « L'utilisation des mégadonnées pouvant porter atteinte non seulement à la vie privée et à la protection des données de façon individuelle, mais également à la dimension collective de ces droits, les politiques préventives et l'évaluation des risques doivent tenir compte de l'impact juridique, social et éthique de cette utilisation, y compris au regard du droit à l'égalité de traitement et à la non-discrimination ».

developed and implemented in a way that protects societies from ideological polarization and algorithmic determinism ».

• Enfin, soulignons une distinction importante en *machine learning* : le système peut être à visée descriptive ou prédictive. Un modèle descriptif décrit sous une forme compréhensible la relation (c'est-à-dire la formule mathématique ou les règles logiques) entre les données à caractère personnel d'une personne et la réponse recherchée. Il a pour but de mieux comprendre cette relation, par exemple, lorsqu'un médecin cherche à comprendre comment et pourquoi une maladie apparaît chez certains patients et pas les autres. Par opposition, un modèle prédictif a pour seul but de prédire la réponse recherchée pour un individu spécifique. Ainsi, tel et tel symptômes présentés par une personne, les données socio-économiques de cette personne, ses habitudes de déplacement, ses données génétiques peuvent conduire à une inférence statistique tirée du rapprochement au sein d'une mégadonnée à prédire le risque de survenance dans les cinq ans de la maladie d'Alzeihmer.

Les applications de l'IA à l'appui de la régulation sont nombreuses. L'analyse instantanée de quantité de textes ou d'images permise par les systèmes d'IA autorise une détection automatique des contenus, en particulier leur caractère xénophobe, raciste, leur caractère de *fake news.* Cette détection des contenus permet également de prévenir l'accès à des copies illicites, même partielles, d'œuvres musicales ou textuelles ou, pour des moteurs de recherche, de bloquer, à la suite de demandes de déférencement, des liens vers des sites reprenant des informations jugées illicites au regard du RGPD(364). Dans tous ces cas, l'IA sert alors d'outil de détection, de filtrage, de déclassification, de déréférencement, de « déprioritisation » ou de blocage à l'appui d'une autorégulation ou d'une législation(365). On peut imaginer d'autres applications : l'IA sert alors d'outil améliorant l'application de la loi. Les autorités fiscales et de sécurité sociale utilisent les

(364) Voy., à ce propos, l'arrêt de la CJUE du 24 septembre 2019 (*Google c. CNIL*, C-507/17 [espèce I]), qui oblige les plateformes offrant des services de moteur de recherche à déférencer les sites qui contiennent des informations, y compris journalistiques, relatives à des données sensibles dépassées depuis le moment de leur publication : « Compte tenu des responsabilités, des compétences et des possibilités de l'exploitant d'un moteur de recherche en tant que responsable du traitement effectué dans le cadre de l'activité de ce moteur, les interdictions et les restrictions prévues à l'article 8, paragraphes 1 et 5, de la directive 95/46 ainsi qu'à l'article 9, paragraphe 1, et à l'article 10 du règlement 2016/679 ne peuvent […] s'appliquer à cet exploitant qu'en raison de ce référencement et, donc, par l'intermédiaire d'une vérification à effectuer, sous le contrôle des autorités nationales compétentes, sur la base d'une demande formée par la personne concernée ». Sur cette décision de la Cour européenne depuis relayée par treize arrêts du Conseil d'État français, lire T. Leonard et Y. Poullet, « L'intérêt général comme arbitre du débat Vie privée *vs* Liberté d'expression », in Y. Poullet (dir.), *Vie Privée, transparence et démocratie*, Actes du colloque du REHNAM, Namur, le 28 novembre 2019, *Cahier du CRIDS*, n° 50, 2020 (à paraître), en particulier, le numéro 26 qui décrit le risque, ici aussi, d'une délégation aux plateformes privées de juger, grâce à l'IA, du déréférencement ou non d'un site.

(365) Sur ce point, lire l'étude déjà citée de C. Marsden et T. Meyer pour le compte de l'European Parliamentary Research Service (EPRS) et la STOA (Scientific Foresight Unit), *Regulating Disinformation with Artificial Intelligence*, EPRS, European Parliamentary Research Service Scientific Foresight Unit (STOA) PE 624.279 – March 2019, qui analyse ces diverses possibilités dans les différents textes portant sur le contrôle des contenus des messages circulant sur le Net.

ressources de l'IA pour lutter contre la fraude fiscale ou à la sécurité sociale ; les services policiers analysent, quant à eux, les risques d'infractions grâce à de tels outils ; contrôlent les mouvements dans les espaces publics ou repèrent les terroristes aux douanes grâce à des systèmes de reconnaissance faciale(366). Quelques affaires aux États-Unis illustrent l'utilisation de systèmes d'IA par les tribunaux pénaux pour calculer les risques de récidive, et est évoqué le remplacement des juges par des systèmes d'IA à la suite des exemples chinois et lettons(367). On conçoit dès lors l'intérêt marqué des régulateurs de promouvoir ou d'imposer le recours à la technologie de l'IA, capable d'une plus-value d'effectivité bien plus importante et dans des domaines plus sensibles encore que les technologies classiques. Cependant, si tel est le cas, les risques liés à l'utilisation de l'IA rappelés ci-dessus sont également plus cruciaux. S'ajoute à ces risques le fait que la non-transparence du fonctionnement des systèmes pourrait entraîner une perte de confiance des personnes soumises aux traitements opérés par l'IA. Une autre préoccupation concerne le fait que l'automatisation galopante des processus de décision engendre une acceptation quasi automatique de la validité et de la pertinence de ces décisions et, corrélativement, un désinvestissement et une déresponsabilisation de décideurs « humains »(368).

21. La régulation des IA, par le législateur et, au-delà, par la régulation au sens large. Amener la confiance dans le fonctionnement des systèmes d'IA est le maître mot du rapport et des lignes directrices proposées par le Groupe d'experts de haut niveau nommés par la Commission en juin 2018 et dont sont issues les *Lignes directrices en matière d'éthique pour une IA digne de confiance* publiées le 8 avril 2019. Le même jour, la Commission lançait une phase pilote « afin de faire en sorte que les lignes directrices en matière éthique pour le développement de l'intelligence artificielle (IA) puissent être mises en œuvre dans la pratique » et invitait les entreprises et pouvoirs publics à adopter ces lignes directrices. Ces lignes directrices affirment trois principes : la licéité, le caractère éthique et, enfin, la robustesse. Elles consacrent sept éléments dits « essentiels » pour parvenir à une IA digne de

(366) Sur le projet d'utilisation des systèmes de reconnaissance faciale mis en place aux frontières européennes, à savoir le système I-Border Ctrl actuellement développé par l'Europe pour le contrôle des frontières, dont les modules sont décrits comme suit par le rapport d'Algorithmwatch et de la fondation Bertelsman (*Automating Society Taking Stock of Automated Decision-Making in the EU*, *A report by AlgorithmWatch in cooperation with Bertelsmann Stiftung*, Étude sponsorisée par l'Open Society Foundations, janvier 2019).

(367) Sur la « justice prédictive » ou le remplacement des juges par les robots, lire entre autres : D. Mougenot et L. Gerard, « Justice robotisée et droits fondamentaux », in Actes du colloque du 8 juin 2018 organisé par le CRIDS de l'Université de Namur : *Le juge et l'algorithme : juges augmentés ou justice diminuée*, Bruxelles, Larcier, 2019 ; D.J. Steinbock, « Data matching, data mining, and due process », *Georgia Law Review*, 2005, p. 61, et D. Kehl, P. Guo et S. Kessler, « Responsive communities, algorithms in the criminal justice system: assessing the use of risk assessment in sentencing », disponible en ligne : https://dash.harvard.edu/bitstream/handle/1/33746041/201707_responsivecommunities_2.pdf?sequence=1.

(368) À cet égard, les experts AI de la Commission relèvent que « *the results produced by the machine, using more and more sophisticated software, and even expert system, has an apparently objective and incontrovertible character to which a human decision-maker may attach too much weight, thus abdicating his own responsibilities* ».

confiance : « Une IA digne de confiance devrait respecter toutes les législations et réglementations applicables ainsi qu'une série d'exigences ; des listes d'évaluation spécifiques visent à faciliter la vérification du respect de chacune de ces exigences :

22. Facteur humain et contrôle humain : les systèmes d'IA devraient être les vecteurs de sociétés équitables en se mettant au service de l'humain et des droits fondamentaux, sans restreindre ou dévoyer l'autonomie humaine.

23. Robustesse et sécurité : une IA digne de confiance nécessite des algorithmes suffisamment sûrs, fiables et robustes pour gérer les erreurs ou les incohérences dans toutes les phases du cycle de vie des systèmes d'IA.

24. Respect de la vie privée et gouvernance des données : il faut que les citoyens aient la maîtrise totale de leurs données personnelles et que les données les concernant ne soient pas utilisées contre eux à des fins préjudiciables ou discriminatoires.

25. Transparence : la traçabilité des systèmes d'IA doit être assurée.

26. Diversité, non-discrimination et équité : les systèmes d'IA devraient prendre en compte tout l'éventail des capacités, aptitudes et besoins humains, et leur accessibilité devrait être garantie.

27. Bien-être sociétal et environnemental : les systèmes d'IA devraient être utilisés pour soutenir des évolutions sociales positives et renforcer la durabilité et la responsabilité écologique.

28. Responsabilisation : il convient de mettre en place des mécanismes pour garantir la responsabilité à l'égard des systèmes d'IA et de leurs résultats, et de les soumettre à une obligation de rendre des comptes ».

Il n'est pas exclu qu'à la suite de ces lignes directrices, l'Union européenne légifère en matière d'IA selon, en tout cas, la promesse de la présidente de la Commission, à peine nommée. Notre propos se limite ici à esquisser quelques principes mis en évidence par quelques régulations européennes déjà étudiées et qui, dès maintenant, entourent le développement et l'utilisation des systèmes IA. On cite : premièrement, la conformité à la loi ; deuxièmement, la transparence ou du moins l'intelligibilité ; troisièmement, le dernier mot à l'humain ; quatrièmement, la nécessité d'une évaluation et d'une réflexion pluridisciplinaire ; la cinquième, la responsabilisation des concepteurs et des fournisseurs au-delà des utilisateurs. Ces réflexions se retrouvent de manière plus ou moins affirmée dans les textes analysés.

29. La conformité. Cette exigence est la première réclamée par le Groupe d'experts de haut niveau dans leurs recommandations (voy. n° 22). Elle a également été soulignée (*supra*, n° 18) à propos de la demande prescrite par l'article 17 de la directive « Droit d'auteur dans le marché unique numérique » de mettre sur pied des mesures de détection et de blocage des copies illicites d'œuvres(369). Au-delà du

(369) À noter, en outre, les discussions de la 4e réunion relative aux mesures prises par les plateformes en matière de systèmes automatiques anti-copies (art. 17 de la directive), tenue le 16 décembre à Bruxelles, où était dénoncée l'utilisation de systèmes soi-disant anti-copies à des fins autres que la finalité légale autorisée : « *According to the European Consumer Organisation (BEUC),*

respect de la loi, on cite la déclaration de mai 2019 de la Commission européenne qui fait suite aux recommandations du Groupe d'experts « *AI applications should not only be consistent with the Law but also adhere to ethical principles* ».

30. La transparence ou, à défaut, l'intelligibilité des décisions prises. C'est sans doute la réclamation la plus forte, mais également la plus difficile à réaliser au vu de la complexité et de l'imprévisibilité du fonctionnement de certains systèmes de *machine learning*, en particulier de *deep learning*. Elle est pourtant une condition du respect de l'autonomie humaine et des libertés des personnes, y compris morales. Toute personne doit pouvoir comprendre les raisons des décisions prises par la machine. Le RGPD exige ainsi une information de la personne concernée de la « logique » des décisions ayant pour seul fondement un traitement automatisé, de même que l'accès à cette « logique »[370]. La directive sur le droit d'auteur prévoit de même (art. 17.8) : « Les États membres prévoient que les fournisseurs de services de partage de contenus en ligne fournissent aux titulaires de droits, à leur demande, des informations adéquates sur le fonctionnement de leurs pratiques en ce qui concerne la coopération visée au paragraphe 4 et, en cas d'accords de licence conclus entre les fournisseurs de services et les titulaires de droits, des informations sur l'utilisation des contenus couverts par les accords ». Le règlement de l'Union européenne n° 2019/1150 du 20 juin 2019 promouvant l'équité et la transparence pour les entreprises utilisatrices de services d'intermédiation en ligne (*J.O.U.E.*, L 186/57 du 11 juillet 2019)[371] instaure également de nombreuses obligations d'information

implementation of article 17 will lead to more false positives (i.e. unjustified blocking). BEUC suggested the Commission should introduce sanctions for repeated false notices by copyrightholders and to make platforms liable for ACR technology failures. On removals following notices, Harvard University academics presented the results of several research reports on errors and misuses or abuses of the US notice-and-takedown procedure, which enables website operators to qualify for the safe harbour under the US Digital Millennium Copyright Act. These include false statements, failed application of copyright exceptions, notices that did not comply with legal requirements and misuse of the system to achieve removals motivated by reasons other than copyright ».

(370) Les articles 13.2 (f) et 14.2 (g) du RGPD mentionnent parmi les informations à communiquer à la personne concernée : « l'existence d'une prise de décision automatisée, y compris un profilage […] et, au moins en pareils cas, des informations utiles concernant la logique sous-jacente, ainsi que l'importance et les conséquences prévues de ce traitement pour la personne concernée ». L'article 15.1 (h) prévoit que l'accès s'étendra aux mêmes informations.

(371) En matière de classement des sites par les services d'intermédiation en ligne, l'article 5 du règlement européen n° 2019/1150 du 20 juin 2019 promouvant l'équité et la transparence pour les entreprises utilisatrices de services d'intermédiation en ligne (*J.O.U.E.*, L 186/57 du 11 juillet 2019) prescrit diverses informations dues aux entreprises utilisatrices des services d'intermédiation : « 1. Les fournisseurs de services d'intermédiation en ligne indiquent dans leurs conditions générales les principaux paramètres déterminant le classement, et les raisons justifiant l'importance relative de ces principaux paramètres par rapport aux autres paramètres. 2. Les fournisseurs de moteurs de recherche en ligne indiquent les principaux paramètres qui, individuellement ou collectivement, sont les plus importants pour déterminer le classement ainsi que l'importance relative de ces principaux paramètres, en fournissant une description facilement et publiquement accessible, énoncée dans une formulation claire et compréhensible, sur les moteurs de recherche en ligne de ces fournisseurs. Ils tiennent cette description à jour. 3. Lorsque les principaux paramètres incluent la possibilité d'influer sur le classement contre toute rémunération directe ou indirecte versée par les entreprises utilisatrices ou les utilisateurs de sites internet d'entreprise au fournisseur concerné, ce fournisseur présente également une description de ces possibilités et des effets de

aux services d'intermédiation en ligne à propos des critères et des décisions prises en matière de *ranking* des sites des utilisateurs de leurs plateformes. Enfin, ce souci de la transparence est largement reconnu par le *Code of Practice on Disinformation* dans pas moins de quatre dispositions qui insistent sur la nécessité pour les internautes de pouvoir comprendre le mode de décision du système automatisé qui préside au blocage, au déclassement ou à la « déprioritisation » d'un site ou message(372).

31. Le dernier mot à l'humain. L'article 22.3 du RGPD est volontiers cité à cet égard. Il oblige le responsable du traitement « à mettre en œuvre des mesures appropriées pour la sauvegarde des droits et libertés et des intérêts légitimes de la personne concernée, au moins du droit de la personne concernée d'obtenir une intervention humaine de la part du responsable du traitement d'exprimer son point de vue et de contester la décision ». Ce même souci de ne pas laisser à la décision de la machine la compétence d'avoir le dernier mot et de mettre en place un organe

cette rémunération sur le classement, conformément aux exigences énoncées aux paragraphes 1 et 2. […] 5. Les descriptions visées aux paragraphes 1, 2 et 3 sont suffisantes pour que les entreprises utilisatrices ou les utilisateurs de sites internet d'entreprise puissent acquérir une compréhension suffisante pour déterminer si, et dans l'affirmative, comment et dans quelle mesure le mécanisme de classement tient compte des éléments suivants […] ».

(372) Voy. le document déjà cité et, en particulier, les dispositions 8, 9 et 10 du Code : « *8. The Signatories of this Code recognize that transparency should be ensured with a view to enabling users to understand why they have been targeted by a given political or issue-based advertisement; 9. Such transparency should reflect the importance of facilitating the assessment of content through indicators of the trustworthiness of content sources, media ownership and verified identity. These indicators should be based on objective criteria and endorsed by news media associations, in line with journalistic principles and processes; 10. The signatories recognize the ongoing legislative work to develop standards for transparency about the main parameters of ranking included in the draft Platform to Business Regulation as well as the work being carried out by the EU Artificial Intelligence Expert Group as well as the EU consumer acquis* ».

Sur le même thème de la désinformation, on se réfère également aux conclusions du rapport : « *Regulating disinformation with artificial intelligence* », déjà cité. Ce rapport conclut (pp. 64 et s.) : « 1 *This study argues that options to ensure independent appeal and audit of platforms' regulation of their users be introduced as soon as feasible. When technical intermediaries need to moderate content and accounts, detailed and transparent policies, notice and appeal procedures, and regular reports are crucial. It is believed this is also valid for automated removals. 2 This study advises against regulatory action that would encourage increased use of AI for content moderation purposes, without strong human review and appeal processes. 3 There is scope for standardizing (the basics of) notice and appeal procedures and reporting, and creating a self-regulatory multistakeholderbody, such as the UN Special Rapporteur's suggested 'social media council'. As recommended by the Special Rapporteur, this multistakeholderbody could, on the one hand, have competence to deal with industry-wide appeals and, on the other hand, work towards a better understanding and minimisationof the effects of AI on freedom of expression and media pluralism. It is believed this would best fit Option 3 classification. 4 This study emphasizes that disinformation is best tackled through media pluralism and literacy initiatives, as these allow diversity of expression and choice. Source transparency indicators are preferable over (de)prioritization of disinformation, and users need to be given the opportunity to understand how their search results or social media feeds are built, and edit their search results/feeds where desirable. 5 Finally, noting the lack of independent evidence or even detailed research in this policy area, the risk of harm remains far too high for any degree of regulatory certainty. The authors reiterate that far greater transparency must be introduced into the variety of AI and disinformation reduction techniques used by online platforms and content providers* ».

de « *fast-checking* » composé de personnes en chair et en os, indépendantes par ailleurs, qui puisse *in fine* se prononcer soit en cas de contestation d'une information considérée comme « désinformation », dans le cadre du Code sur la désinformation(373), soit en cas de contestation sur le *ranking* d'un site, dans le cadre du Règlement sur l'équité et la transparence des entreprises utilisatrices de services d'intermédiation en ligne(374), soit de blocage d'une copie illicite, dans le cadre de la directive sur le droit d'auteur(375).

32. L'évaluation et, si possible, interdisciplinarité. Le besoin d'une évaluation de la conformité et de l'effectivité des systèmes d'IA est un *leitmotiv* des textes cités. À propos de la directive sur le droit d'auteur, cette évaluation par les *stakeholders*, c'est-à-dire les associations de consommateurs et d'auteurs, et les plateformes est prévue explicitement(376). Récemment, le 16 décembre 2019, s'est tenue la 4e réunion relative aux mesures prises par les plateformes en matière de systèmes automatiques anti-copies illicites. À noter un point de ses conclusions : « *Anti-piracy agencies agree that the state of art of technology is not sufficiently effective to apply ACR systems*

(373) Voy. la disposition n° 12 : « *Relevant Signatories commit to support good faith independent efforts to track Disinformation and understand its impact, including the independent network of fact-checkers facilitated by the European Commission upon its establishment* ». Voy. égal. l'affirmation reprise dans les conclusions du rapport Marsden *et al.*, rapport rédigé pour le Parlement européen (cité note 300), en particulier le point 3 de la citation.

(374) Voy. les articles 11 et 12 du Règlement déjà cité. L'article 11 oblige à la mise sur pied d'un système interne de traitement des plaintes : « Les fournisseurs de services d'intermédiation en ligne mettent à disposition un système interne de traitement des plaintes émanant des entreprises utilisatrices. Ce système interne de traitement des plaintes est facilement accessible et gratuit pour les entreprises utilisatrices et garantit un traitement dans un délai raisonnable. Il est fondé sur les principes de transparence et d'égalité de traitement entre situations équivalentes et il traite les plaintes d'une manière proportionnée à leur importance et à leur complexité. Il permet aux entreprises utilisatrices de déposer directement auprès du fournisseur concerné des plaintes. Les fournisseurs de services d'intermédiation en ligne mettent à disposition un système interne de traitement des plaintes émanant des entreprises utilisatrices ». L'article 12 concerne la nécessité, pour les services d'intermédiation en ligne, de référer des médiateurs indépendants : « Les fournisseurs de services d'intermédiation en ligne indiquent dans leurs conditions générales deux ou plusieurs médiateurs avec lesquels ils sont prêts à prendre contact en vue de parvenir à un accord avec les entreprises utilisatrices sur le règlement extrajudiciaire de tout litige entre le fournisseur et une entreprise utilisatrice en relation avec la fourniture des services d'intermédiation en ligne concernés, y compris les plaintes qui n'ont pu être résolues dans le cadre du système interne de traitement des plaintes visé à l'article 11 ».

(375) Voy. l'article 17.8 de la directive : « Les États membres prévoient la mise en place par les fournisseurs de services de partage de contenus en ligne d'un dispositif de traitement des plaintes et de recours rapide et efficace, à la disposition des utilisateurs de leurs services en cas de litige portant sur le blocage de l'accès à des œuvres ou autres objets protégés qu'ils ont téléversés ou sur leur retrait ».

(376) Voy. l'extrait d'un rapport à la suite de cette 4e réunion. « *At fourth meeting on article 17 of the EU copyright Directive, stakeholders discuss issues in the application of automatic content recognition systems. Music collecting societies and sports rights organisations called on platforms to increase transparency regarding the policies they apply to the use of their proprietary automated content recognition (ACR) systems. Facebook explained that certain policies aim to prevent rightsholders from abusing its ACR system. Anti-piracy agencies agree that the state of art of technology is not sufficiently effective to apply ACR systems without any human review. They say that collecting societies face difficulties in collaborating with platforms not because of technology itself but because of the platforms' policies on the use of their ACR systems, which are not transparent and change frequently* ».

without any human review ». Le RGPD approche différemment la question de l'évaluation dans la mesure où il considère que ces systèmes de décision fondée sur la technologie AI constituent des traitements à haut risque et exigent donc une évaluation des risques courus par les libertés individuelles, une justification des solutions prises et la consultation de l'autorité de protection des données. Ainsi, l'article 35 du RGPD impose l'obligation au responsable de traitement de procéder à une « analyse d'impact » du traitement projeté lorsque celui comporte un « risque élevé » pour les personnes concernées. Cette exigence est due en particulier, « en cas d'évaluation systématique et approfondie d'aspects personnels concernant des personnes physiques, qui est fondée sur un traitement automatisé y compris le profilage », lorsque des décisions sont prises sur la base de cette évaluation ayant des effets juridiques sur les personnes concernées ou les affectant de manière significative.

Cette évaluation devrait être le fait d'un organe réunissant des représentants des différents intérêts. En matière de régulation des contenus et de la lutte contre la désinformation, le rapport Marsden *et alii* de la STOA(377) conclut à la nécessité de ce contrôle par un organe d'autorégulation *multistakehoder* : « *There is scope for… creating a self-regulatory multistakeholder body, such as the UN Special Rapporteur's suggested 'social media council'. As recommended by the Special Rapporteur, this multistakeholder body could, on the one hand, have competence to deal with industry-wide appeals and, on the other hand, work towards a better understanding and minimization of the effects of AI on freedom of expression and media pluralism* ». Pour les systèmes IA développés par ou pour les administrations et autorités publiques, le rapport anglais « *Regulating in a digital World* »(378) préconise le recours à un audit régulier par l'autorité publique qui disposerait d'un centre d'évaluation des systèmes IA, centre de test et d'audit géré de manière indépendante de l'État. Ce centre devrait également veiller à améliorer l'expertise des organismes qui conçoivent les systèmes IA utilisés par l'autorité et son administration. Il fixerait les procédures et modalités, tant organisationnelles que techniques, les possibilités offertes aux citoyens afin de contester les décisions prises sur la base des systèmes IA. L'initiative recommande aux agences publiques de répertorier et de décrire les systèmes de décision automatisés, y compris d'évaluer leurs portée et impact. Elle recommande également de mettre en place des modalités d'accès afin que des chercheurs, des experts indépendants, des associations ou des journalistes puissent accéder et évaluer ces systèmes et, pour cela, préalablement de s'assurer notamment que leurs fournisseurs privés de systèmes acceptent ces vérifications.

33. La responsabilisation élargie. Au cas où le fonctionnement du système d'IA aboutirait à des décisions inappropriées ou dommageables pour les individus concernés, la cause n'est pas nécessairement à rechercher du côté de l'entreprise ou

(377) Rapport T. Marsden *et al.*, *Regulating disinformation with artificial intelligence*, STUDY Panel for the Future of Science and Technology European Science-Media Hub EPRS (European Parliamentary Research Service), 2019, pp. 64 et s. (pour les références de ce rapport, voy. notre note n° 41).
(378) Rapport du Select Committee on Communications, *Regulating in a Digital World*, 2nd Report of Session 2017-2019, House of Lords, 9 mars 2019.

de l'administration qui utilise un tel système(379). Le concepteur de l'algorithme peut en être le responsable par les biais qu'il a introduits ou permis d'introduire, les fournisseurs des données de test ou des *big data* peuvent également être à l'origine de ce mauvais fonctionnement. En matière de protection des données, le RGPD ne prévoit pas d'extension de la responsabilité à ces professionnels. C'est un reproche que lui adresse le Comité consultatif de la Convention n° 108 lorsqu'elle publie les « Lignes directrices sur les Mégadonnées » du 23 janvier 2017 souhaitant que ces derniers puissent également voir leurs responsabilités engagées(380).

Conclusions

34. Quelques réflexions. Entre une autorégulation sauvage et une réglementation tatillonne, l'Europe choisit la voie de la corégulation. Sans doute, cette corégulation est-elle à degré variable ? Le RGPD – mais l'exemple est loin d'être unique – constitue une parfaite illustration de corégulation descendante. Les balises que le RGPD impose sont très détaillées et laissent peu de place à une véritable innovation. Il nous paraît que l'autorégulation que présente le *Code of Practice on Disinformation* évolue lentement, mais sûrement, vers une corégulation ascendante sur la pression de plus en plus grande des autorités européennes à la suite de leur prise de conscience de l'impact sur la société et sur les individus des plateformes, également qualifiées de services d'intermédiation en ligne.

Mettre la technologie au service d'une régulation conforme au Droit et légitime est un autre défi. La technologie, en particulier de l'intelligence artificielle, apparaît comme un outil merveilleux d'effectivité de la régulation, mais cet outil ne peut être conforme et légitime que si la délégation donnée à ceux qui le mettront en place est placée sous le contrôle d'organes multidisciplinaires, suffisamment indépendants et experts. Ce contrôle n'est pas simple vu l'opacité du fonctionnement des applications d'intelligence artificielle et la volonté, sans doute trop confiante, de leur reconnaître

(379) Au moment où nous écrivions ces lignes, nous prenions connaissance de l'existence du rapport : « *Liability for Artificial Intelligence and Other Emerging Digital Technologies* », préparé par l'Expert Group on Liability and New Technologies Formation, décembre 2019. Le rapport est disponible à l'adresse suivante : https://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupMeetingDoc&docid=36608.

(380) « Là où le RGPD et la Convention 108+ ne mentionnent que les obligations du "responsable" du traitement, les deux Lignes directrices ajoutent la responsabilité d'autres acteurs intervenant soit dans la fourniture des mégadonnées (*big data*) ou bibliothèques (*libraries*) qui serviront aux systèmes de profilage, soit dans la conception et la mise en œuvre des algorithmes de base ou l'adaptation de ces algorithmes aux besoins particuliers d'un secteur ou d'un système particulier. On ne s'étonne pas de ce souci tant l'analyse des acteurs montre bien que les qualités du traitement et l'étendue des risques y liés sont loin de dépendre du seul responsable du traitement et trouvent leurs explications dans le choix des données souvent acquises à l'extérieur (le fournisseur de données), le choix de l'algorithme de base ou adapté par un tiers aux besoins de l'application spécifique du responsable (les développeurs et fabricants, selon l'expression des lignes directrices IA) ». (Y. Poullet et B. Frenay, *Rapport et propositions de recommandations sur le « Profilage et la Convention 108+ du Conseil de l'Europe »*, *op. cit.*, p. 22). Voy., toutefois, notre remarque (note 342), à propos des *Guidelines* de l'EDPB à propos des principes de « *privacy by design et by default* ».

une autonomie de décision. Nous avons plaidé pour que l'homme reste maître de la machine et puisse lui faire confiance. Pour ce faire, il est clair que son combat ne peut être individuel, mais doit être collectif. Sa maîtrise passe indiscutablement par un renforcement de l'autorité publique, au moment même où la puissance des GAFAM met en cause de manière cruciale leur souveraineté. Se réapproprier cette souveraineté ne signifie pas le rejet de l'autorégulation ou de la corégulation, mais, certainement, l'exigence de leurs conformité et légitimité. Cela signifie la réaffirmation du Droit, pas seulement celui des libertés individuelles, mais également de la concurrence et du droit de la consommation.